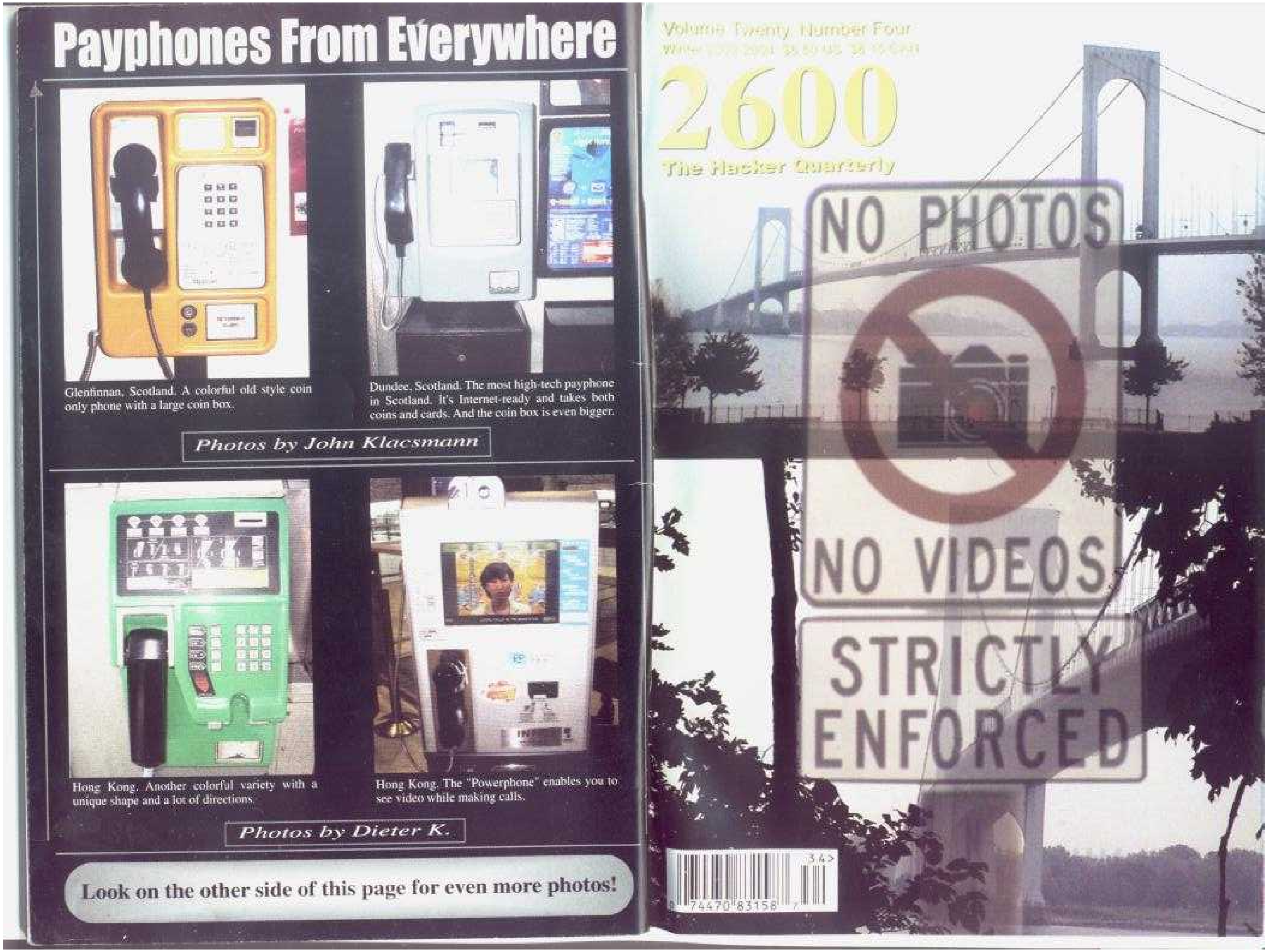
2600 Magazine – Volume 20, Number 4



Payphones From Everywhere

Glenfinnan, Scotland. A colorful old style coin only phone with a large coin box.

Dundee, Scotland. The most high-tech payphone in Scotland. It's Internet-ready and takes both coins and cards. And the coin box is even bigger.

Photos by John Klacsmann

Hong Kong. Another colorful variety with a unique shape and a lot of directions.

Hong Kong. The "Powerphone" enables you to see video while making calls.

Photos by Dieter K.

Look on the other side of this page for even more photos!

Volume Twenty, Number Four

Winter 2003-2004 $5.50 US $8.15 CAN

2600

The Hacker Quarterly

> "No one realized that the pumps that delivered fuel to the emergency generators were electric."
>
> \- Angel Feliciano, representative of Verizon workers explaining why Verizon's backup power failed during the August 14 blackout causing disruption to the 911 service.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Photos
Rebel

Cover Design
Dabu Ch'wald

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dalai, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, David Ruderman, Screamer Chaotix, Seraf, Silent Switchman, Mr. Upsetter

Webmasters: Juintz, Kerry

Network Operations: css, mlc

Broadcast Coordinators: Juintz, Pete, daRonin, Digital Mercenary, Kobold, w3rd, Gehenna, Brilldon, Chibi-Kim, lee, Nico, Logix, Boink, John

IRC Admins: Antipent, daRonin, Digital Mercenary, Shardy, The Electronic Delinquent

Inspirational Music: Makem & Clancy, Fun Lovin' Criminals, Electric Hellfire Club, Mekons, Elliot Smith, Marvin Pontiac

Shout Outs: Tommy Chong

*2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.
2 Flowerfield, St. James, NY 11780.
Periodicals postage paid at
St. James, NY and additional offices.*

POSTMASTER:
Send address changes to
2600, P.O. Box 752, Middle Island,
NY 11953-0752.
Copyright (c) 2003
2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada
- $20 individual,
$50 corporate (U.S. funds).
Overseas - $30 individual,
$65 corporate.
Back issues available for 1984-2002 at
$20 per year,
$26 per year overseas.
Individual issues available from 1988 on
at $5.00 each, $6.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752
(subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631-474-2677**

Data

PARANOIA

Sanity

What have we learned from publishing a hacker magazine for the past 20 years?

Quite a bit actually.

We've learned that when given the chance, paranoia has a way of taking root and dominating even the most minor of crises. From Day One we've had to deal with morons who just don't understand what the hacker culture is all about and who have always seen us as a threat comparable to their worst nightmare. And this *always* fed on ignorance of the unknown and of the very great desire *not* to learn anything that may have run counter to their initial perceptions.

At first it was a bit funny. Some of us even thought it was fun to be perceived as an all knowing, all powerful enemy. Imagine, teenagers with the ability to make large corporations and annoying system administrators cower in fear! Never mind that the fear was mostly misplaced. To many of us, it was all a big game.

But then the paranoia began to take hold in ways that were hard to ignore. People began to actually go to prison for accessing computer systems without authorization or for simply making free phone calls. Few denied at the time that these were transgressions. But prison? It all seemed so absurd.

But we got used to it. And in so doing, an important turning point was reached. Hackers were no longer just kids playing around. In the eyes of mainstream society, hackers had become definable as actual criminals, along with thieves, murderers, rapists, etc. In some cases hackers were viewed with *more* fear than violent criminals and even received greater sentences. And again it seemed incredibly absurd. While such abuse and illogical thinking proved to be a lot harder for us to get used to, a good number of politicians, judges, and members of law enforcement seemed to have no trouble with the concept. They could envision sending a hacker to prison for life for crimes that in the real world would hardly merit an overnight stay in the county jail.

Why the imbalance? Again, it always comes back to ignorance. When you don't understand a particular group of people, you're all the more likely to attribute skills and motives to them that have absolutely no basis in reality. This of course is nothing new. What *is* new now are the tools being used. The implications for their misuse and control by those who don't share our passion for free speech, free association, dissent, and numerous other liberties we've fought long and hard for over the centuries are simply unprecedented.

And again, we are on the verge of getting used to it.

Today, nearly 20 years to the day after *2600* printed its first issue, we live in a very different world. The things we took for granted in 1984 (ironically enough) simply don't hold true now. We currently live in a society of barriers. Our leaders have to be kept away from the people because of what we could potentially do to them. Great barricades must be erected in front of buildings we once entered freely because they could be considered "targets" of an elusive and faceless foe. We know little of who they are and how they will strike so the fear becomes all the stronger. Familiar? Of course, because these strategies have been used countless times before. Even if we haven't been paying any attention at all to what's been going on throughout history, a quick look at the popular culture of television and movies will reveal precisely these tactics as the ones of choice for anyone trying to control a populace and use their own fear as a weapon of reinforcement.

So shouldn't it be easy to see the threat and to take the necessary measures to keep it from destroying us? Only if we take a couple of steps back and see where we're going without being enveloped in the fear and paranoia that seem to have taken over all elements of our society in recent years. Sometimes this involves looking at a different culture and realizing how alternative ways of handling situations may be a better idea. Or it may involve taking yourself back to the period we all mistake for "a simpler time" when these problems didn't define our lives. Things have always been complex. What's changed are the tools and the priorities. We have technology today that can be used for great good or horrific evil, that can allow us to share information and data of all sorts or be relentlessly tracked and monitored by the authorities of the world in the name of safety and security.

The danger lies in accepting what we're told without question along with the perception that anyone who stands up to the system is somehow a threat to all of us. There are many people reading *2600* now who weren't even born when we started publishing. They have never experienced what so many others have. And this trend will continue. If nothing changes, the children of tomorrow will only know a nation of orange alerts, hostility to foreigners, endless warfare against an unseen enemy, curtailment of civil liberties to anyone considered an enemy of the state, and fear that never goes away.

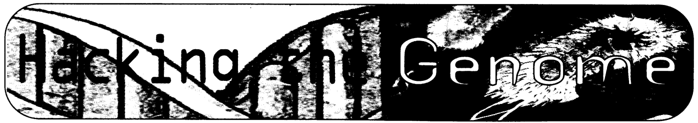
Why would anyone want a society like this? For the same reason that those first changes we noticed years ago were implemented. Control is like an addiction. Those in control want desperately to cling to it and to be able to strike out at those they don't understand or see as some sort of potential threat. We saw that attitude as affecting hackers because that was the world we were a part of. Now it's a lot easier to see it affecting so many more.

But hackers have had the opportunity to gain a unique perspective. We understand both the good and the bad in technology. We're not afraid to bend the rules to learn how something works, despite the increasingly severe penalties suffered by those who dare. We can apply this knowledge over society and see the inherent risks involved in the latest ideas put forth by the Homeland Security people to weed out the "evildoers" among us. We can see the threats posed by such things as electronic voting systems that don't rely on open source software and are shrouded in secrecy. We can realize how all the barriers and fear tactics in the world will do nothing to stop a truly determined enemy and how such methods will actually do far more harm than good because of the fact that one day we won't know anything else. We can also speak in ways that others can't because we've seen the changes as they affect us specifically and also because we have a history of not blindly accepting what we're told. The fact that many of us understand how technology is being used here adds valuable insight. And it also makes us even more of a threat to those addicted to control.

This clearly won't be a journey for the faint of heart.

As we close the door on our second decade, it's important to note that we have a great deal of optimism for the future, despite all of the gloom and doom around us. Why is this? For the simple reason that we believe the right people are gathering in the right place at the right time. We were happy to learn that a Norwegian appeals court recently upheld a decision clearing the author of the DeCSS program of any charges, despite the wishes of the MPAA and the proponents of the DMCA in this country. In the last couple of years, we've had more people than ever express genuine interest in the workings of technology and in knowing all of the ways it can be used against them by malevolent powers, as well as ways it can be used for something positive. We've seen tremendous attention paid to this at the HOPE conferences and we expect to see even more this July as we do it again. The alertness of our readers, listeners to our radio broadcasts, and attendees of our meetings and conferences has been a tremendous inspiration to us and to so many others. This is what can change things and move us all into a less confining world. We've seen people better their living conditions and improve the societies they live in once it became evident that the old way was not the right way. There's no reason to believe that the road we're going down won't eventually result in that very same realization. And we'll get there by keeping our eyes open and finding friends in the least expected places. That's what's gotten us this far.

Hacking the Genome



by Professor L

The creation of genetically modified organisms (GMOs) is now within the ability of a knowledgeable and dedicated hacker. The most common genetic modification is the insertion of genes from one organism into another. The recipient is called a "transgenic organism" and this article will give you enough information so that anyone who could pass a high school biology lab can create one.

The usual *2600* article starts off with a disclaimer about how the article is for informational purposes only, and should the reader do anything illegal or dangerous, that's the reader's fault. The disclaimer in this article has to be stronger. Creating transgenic organisms has the potential to do great, possibly even catastrophic harm to the entire biosphere. Although the specific manipulations I describe in this article are safe (and often done in biology teaching labs), knowledge of the methods of genetic engineering have the potential to unleash enormous forces for good or for evil.

The most likely harmful consequence of hackers making a mistake with genetic engineering is for the hackers to get sick or to make the people around them sick. Maybe really, really sick. If you are going to try these techniques, learn about safe laboratory practices and follow them. The consequences of screwing up with genetic engineering are much worse than a mere jail sentence, so treat it seriously. No kidding.

If these techniques are so dangerous, why on earth would I want to tell hackers how to use them? I've thought about this long and hard before writing this article, and I have three reasons for writing. First, none of the information in this article is all that hard to find these days. Good high school biology classes teach the ideas (although they often figure out how to make it seem boring), and pretty much every community college will have a molecular biology lab class that teaches all of this information and good lab technique, too. If you think this article is cool, I would strongly encourage you to take a real lab mol bio course and get at the good stuff.

My second reason is that I believe in the hacker mentality. When as a teenager I got tired of stacking tandems with my 8038-based blue box, I built an Imsai 8008, one of the first computer kits. Twenty-five years later, looking at my lab and all the scientific publications and prizes I have, even the straight world would have to admit that some hackers have made positive contributions to society. The hackers in the Homebrew Computer Club in the 70's spawned much of what would become Silicon Valley. The technologies that fascinate us have the power to create a radically different world; that is, they have the potential to be used for both awesome creation and awesome destruction. Hackers, who these days I think of as kids with a thirst for knowledge and the urge to try things for themselves, can be the ones with the powerfully creative ideas about how to use new technologies.

And my third reason for writing is that corporate powers are already using these technologies very broadly, and in ways that I don't feel are doing justice to their potential. With this article, I hope to inspire people to learn about what genetic engineering can do, and to come up with superior alternatives to the profit-seeking corporate approach. How do corporations use genetically modified organisms? Chances are, you are eating them! Pretty much all processed food in America contains GMOs. Monsanto's Roundup Ready crops dominate worldwide commercial agriculture, including soybeans, corn, cotton, canola oil, and sugar. The particular genetic modification in these foods makes it possible to dump the weedkiller Roundup on the crops without killing them. It's convenient for industrial farmers and it helps keep Monsanto the world's largest seller of herbicides. Surely there must be a better use for transgenic organisms that that! I hope someone reading this article will one day invent it.

Now that I have convinced you to be safety conscious and to strive to use this power for good (I did convince you, didn't I?), let's get started on the methods of how new genes are inserted into organisms. First, you will need to know a little bit of terminology. The base organism that we will be adding the genes to is called the "host." The host, like just about all organisms, can be thought of as a machine for turning environmentally available material and energy (food) into copies of itself. One of the key components of any organism is its genome, that is, its complete collection of genes. The genome contains all of the instructions for making the chemicals (mostly proteins) that do the work of transforming food into offspring. We are going to add a new gene, called the "transgene," to the host.

Every organism is made up of cells (adult humans have about one trillion cells; many kinds of organisms consist of only a single cell), and each cell has its own copy of the organism's genome. Both the genome and the transgene are DNA molecules. DNA is a very long polymer, which means it is a molecule made up of a string of repeating components. In the case of DNA, the components are called nucleotides, and referred to by their one-letter abbreviations, A, C, T, and G. The human genome has about three billion nucleotides. The transgene we are going to insert is only a few thousand nucleotides. However, we are not going to learn how to insert new genes into human beings. Not only is that potentially very dangerous (and highly regulated), but inserting genes into all the cells of multicellular organism like a mammal requires better laboratory technique than a first-time genetic engineer is going to be able to achieve. In this article, I will teach you how to put the firefly genes that are responsible for the firefly's glow into Escherichia coli (E. coli for short), the bacterium that lives in your gut. You're going to make intestinal bacteria that glow in the dark.

So, in this article, the host will be E. coli and the transgenes will be the gene from fireflies that make them glow. This gene is called Luciferase (who says scientists don't have a sense of humor?). In order to do your genetic engineering, you will first have to learn how to grow controlled populations of bacteria. Growing bacteria is a lot like keeping any other kind of pet. You need a source of them to start with, you need a home for them that keeps them safe (mostly from other creatures or contaminants), and you need to make sure they have the right kind of food, the right temperature, and so on.

Because cells are too small to see, it helps to have a microscope for this work, although it's not strictly necessary. Bacteria reproduce very quickly and when enough of them grow together (called a colony), they are visible to the naked eye. In order to get started, you need to get some E. coli, some agar-coated petri dishes (their food and home), and loop (a simple thin piece of metal for transporting cells from the source to the dish). You also will need to learn a little about sterile lab procedures so that you don't contaminate your cells. In the sources section at the end of this article, I recommend a kit that you can buy pretty cheaply that has all the materials you need. Eventually, you'll know enough to be able to scrounge all kinds of cool materials for genetic engineering that cost little or nothing, but I'd recommend starting with the kit.

The key task is getting the transgene into the genome of the E. coli. Hosts, of course, have various methods for resisting the addition of foreign DNA. The most basic of these is the cell membrane, which acts like skin for cells. It's the job of the membrane to keep the insides in and the outsides out. However, membranes have to let in food and let out wastes, so they are permeable. In order to get the transgene inside the cell, we have to manipulate it so that it will take up the new genes. For bacteria, figuring out this problem is really the main task in creating a transgenic organism, and it's pretty easy. For higher organisms, there is more structure (the genome stays in an internal structure called the nucleus of the cell) and better defenses against foreign DNA, making the insertion of transgenes more difficult. However, inserting transgenes into higher organisms (including mammals, like mice or monkeys) is routine laboratory procedure these days.

In addition to making the E. coli take in the foreign DNA, we have to make sure that the DNA is treated as if it were the organism's own. In bacteria, this is also fairly easy. Bacteria often exchange small pieces of DNA, called plasmids, with each other. These plasmids are separate from the organism's main

DNA and allow bacteria to exchange beneficial genetic material with each other, even though they don't replicate sexually (sex is nature's best way of exchanging genetic material between organisms). Vector is the name that biologists use for something that can introduce foreign DNA into a cell. Plasmids are good vectors for bacterial hosts. Other vectors that work better for more complex hosts include viruses that have had transgenic payloads grafted into them, or even tiny gold beads coated with DNA that can be shot into a cell with a "gene gun."

The creation of plasmids (or other vectors) with transgenic payloads is made possible by the existence of DNA splicing enzymes. Simple laboratory techniques allow the extraction of naturally occurring plasmids from bacteria and splicing the DNA for the new gene into them. The hardest part is figuring out which combination of genes to insert into a host in order to get a desired effect. However, those techniques are beyond the scope of this introductory article. For our purposes, we can just buy plasmids with our desired genes from a scientific supply house. An E. coli plasmid with the Luciferase gene in it is called pUC18-luxR, and can be purchased from many places (see sources section, below).

Once you have successfully grown some E. coli colonies and purchased your Luciferase plasmid, the process of creating glow-in-the-dark bacteria is pig-easy. You make the bacterial membrane permeable to the plasmid by treating it with a solution of calcium chloride. At this point, the cells are said to be "competent" for transformation and the plasmids can be added. Then let the cells grow at body temperature (37C) for 12-24 hours. Turn out the lights and look at your petri dish - you should be able to see colonies that quite clearly glow in the dark. Congratulations! You've just created your first transgenic organism! The recommended kit has detailed instructions (called a protocol in molecular biology). The protocol can also be downloaded from the net without buying the kit.

Now if this feels too much like the script kiddy version of genetic engineering, then there are lots of other projects you might take on. You can design and construct your own plasmids, perhaps with multiple transgenes. In order to breed pure populations of transgenic bacteria, one often includes an antibiotic resistance gene in the plasmid, and then applies the antibiotic to the petri dishes. Only the bacteria that took up the plasmid will survive, and the evolutionary selective pressure will ensure that the bacteria won't lose the transgenes. In considering which genes to add, you might learn to use GenBank and LocusLink, two important web-accessible databases of genes. Start by looking up green fluorescent protein (GFP). Or buy a GFP transgenic fish from GloFish.

Hacking the genome is the future. You can be there now....

Sources

A complete kit with everything you need to do this experiment is available from Modern Biology, Inc. for less than $75. It is part number IND-9 and you can order it over the web. Visit http://www.modernbio.com/ind-9.htm to see what's in the kit and how to order it. Modern Biology has all kinds of really cool kits that don't require fancy labs or a lot of experience to use. Check out their whole catalog at http://www.modernbio.com/TableOContents.htm. You can see the complete E. coli transgenic protocol (that is, the detailed instructions) for free before you order by reading http://www.terrificscience.org/lessonexchange/PACTPDF/GlowingEcoli.pdf A different $80 kit allows you to extract DNA from any organism (including yourself), which with some DNA splicing enzymes and some additional knowledge of how to recombine bits of DNA, you could then use for creating new plasmids. It's available from the Discovery Channel store as http://shopping.discovery.com/stores/servlet/ProductDisplay?catalogId=10000&storeId=10000&productId=53965. This kit includes an inexpensive centrifuge, which you are going to need if you want to continue your genetic engineering experimentation. You can get good scientific microscopes on eBay or maybe you have one in a basement somewhere. If you're going to work with GFP, you probably want a microscope for fluorescence work; it will have a filter set and high power illumination.

If you would like proof that many of the foods you eat contain genetically modified organisms, you might be interested in the kits available from Investigen, which uses a similar technology for easy detection of many genetically modified organisms. See http://www.investigen.com/products.html for the details. If you want to look up interesting genes that you might want to add to your bacteria, try using GenBank or LocusLink from http://ncbi.nlm.nih.gov. Once you get good at transforming bacteria and want to start thinking about more ambitious transgenic organisms, you should take a look at the offerings from Clontech http://www.bdbiosciences.com/clontech/, Qiagen http://www1.qiagen.com/Products/Transfection/TransfectionReagents/EffecteneTransfectionReagent.aspx?ShowInfo=1, and QBiogene http://www.qbiogene.com/literature/protocols/gene-expression/pdf/p-adeno-express.pdf. Or you can just buy a GFP zebrafish from http://www.glofish.com.

And before you start working on your plan for creating a Luciferase transgenic puppy by doing genetic engineering on your dog, you should probably learn real molecular biology laboratory techniques by taking a class, maybe like this one: http://a32.lehman.cuny.edu/molbio_course/Basic_techniques.htm. Who knows, maybe I'll be your teacher....

Shoutouts: DMcS for taking it seriously and finding the GloFish and the Discovery kit, and to AG Monster for reminding me that although I am old now, I was a hacker once, too.

WHOM Do You Trust?

by Juraj Bednar
ca@jurajbednar.com

"Security is a process," says a common security expression. I would also like to add that security is *about* processes. In this article you will also see how the security of different organizations affects your own security.

Most of the web communication in today's "secure" Internet is protected by a set of protocols defined in standard, called Transport Layer Security (the successor of SSL: Secure Sockets Layer, developed by Netscape). While the protocol itself is quite strong and the data are protected by mostly safe ciphers and technologies, there is one weak point, like in many asymmetric cryptosystems: distribution of keys (or PKI, short for Public Key Infrastructure).

An asymmetric cryptosystem protects its users against a passive attack (sniffing). Using the Diffie-Hellman key exchange or RSA, it is very difficult to eavesdrop on someone's traffic. There is one widely known attack, known as Man in the Middle. Using this technique, the communication channel is being actively attacked. Parties, while thinking they are communicating with each other, are effectively talking to an attacker, who acts as a middleman.

A solution to this is a safe distribution of keys. If both parties know each other's public key, they can safely communicate. So the problem with today's asymmetric cryptosystems is not about ciphers - they are quite strong. It is mostly about key distribution. PKI comes as a solution to this, where communicating parties own only a few public keys of so called Certification Authorities (or CAs). These are trusted third parties, who pick an identity and a public key of a user or organization, put them together and "stamp" them with their digital signature. When you start communication with someone, he presents you with a valid certificate. You (or better your browser - if we are talking about the web) check the digital signature, the name of a party, etc. If you trust the CA that issued the certificate, you can safely communicate. This last "if" is the big one.

When I wanted a certificate for my own website (jurajbednar.com), I did my own research. The result was quite shocking. I was able to trick a lot of them into issuing me a certificate when they really shouldn't have.

The case of RIPE

I was quite shocked when I found an authority which did authorization using a whois registry. The process looks like this: You fill out a form on their web page (of course using plain unprotected http - why would a CA use https?) and submit a CSR (certificate signing request). They'll send you a confirmation e-mail, you click the link and choose which of the contacts (administrative, technical, or zone) they should contact. They send a mail to the contact you choose and after clicking on a link in the e-mail, they issue a signed certificate.

Now, wait a moment. There are some questions to be asked. How is a contact in a whois database meant to authenticate someone over the Internet? How do we know he is authoritative to decide if someone should issue a certificate? Do they know that most domains in RIPE do not have mnt-by entry which protects the contact by password or PGP in order to make changes? Anyone can make changes to contacts without mnt-by. How could an unprotected e-mail that can be sniffed on the way be trusted as a way to determine whether to issue a certificate?

The CA is on http://certs.ipsca.com/. They have quite low prices and even issue free six month certificates. They are in MS Trust Root (happily not in Mozilla), so anyone with MSIE 5.01 or higher trusts them, unless they decided not to. One of my friends who operates an Internet shop wanted an SSL certificate, so I told her that I would try to get one for her. I explained that I was doing some sort of research and I wanted to trick the authority into issuing it without using access to her accounts or web space (I hosted the site for her) and without her or her colleagues helping me. So I could be literally anyone, but in this case that was part of my research. I had the permission, so I did not break the law.

So first, I changed her contact in RIPE (which of course did not have the mnt-by entry) to my e-mail address. I also added the changed line with my address and correct date of change (these are not added automatically by RIPE). The entry was changed by a robot. She did not get an e-mail about this change. Then I generated a key, a CSR, filled out the form, got the mail, and clicked on the link. Then the page said that they could not contact the RIPE registry, so they filled the contacts with hostmaster, postmaster, and webmaster aliases of the particular domain. While I could receive mail for these addresses (I am an administrator of her mail domain), I decided to be cheeky and mailed back with my ticket number. I sent the whois registry entry with all the contacts (including the changed line, which said that I changed the entry the very same day to my own address!). In a few minutes, the contacts on the web page were set to what I mailed them. I chose my e-mail address, got another mail, clicked another link, and the certificate was issued. I installed the certificate for her shop and she was quite happy. I was happy because I used no power over her web space, domain, or any administrative power. In fact, to issue this certificate, I only used one e-mail address. That makes a man in the middle attack quite simple. It cost me no money so if I used some anonymous access (like driving to some random city and using wifi with a changed MAC address), and created mail on some freemail, I would get a certificate, possibly without the domain owners even noticing this.

Actually performing the man in the middle attack when you have a certificate that most web users trust by default is very easy now. You can use Dug Song's excellent dsniff package. You could rob someone's bank account if the target domain was a bank and they did not use man in the middle resistant protection (such as secureID that digitally signs all parameters of transactions and bank processes it only when such signature is filled in). You could snoop on someone's mail account if they use web mail to access it. And as the web page of this CA perfectly states - it is a matter of minutes.

If your registry provides a way to protect entries in the registry (such as RIPE's mnt-by), use it. When I looked at banks in my country (which is otherwise quite advanced in IT), none of them used mnt-by. Protecting your entries is also a matter of minutes. Do it.

The Case of Papers

Even before this CA, I found E-BizID, which acts as a reseller for Comodogroup (which I chose as my own CA later on). They had a 50 percent discount on the certificates that time and also issued 30 day free test certificates (that were signed by the real authority). I had no idea how they authenticated sites, so I filled in a form to get a certificate for my provider's web mail machine that I am an administrator of. It told me to fax the business license to some number. As I filled out the form correctly (stating who owns the machine, full company name and address, etc.) and it was around Christmas, I just let it be. But later on I was having a phone conversation with another administrator from the company and told him that they are quite cheap and they should buy the certificate, protecting their clients. They decided to buy it for another domain name which had the same web mail installed. They paid for it and faxed the business license. We both received the certificate. I got my testing certificate and they got the real one. Quite interesting.

The question to ask is - is faxing a business license a way to authenticate and authorize users? In our country, anyone can obtain anyone's business license in the court office (the court has a database of all business licenses). If you want to do business with someone, you can go there and request a license which will tell you in what field they are permitted to do business, who owns the company, etc. This business license (here called "transcript from business registry") is the same as the company owners get. There is no difference. Anyone can get it. That means anyone can fax it. That means anyone can get a certificate.

If this was not the case, I wonder how an American CA could determine if the paper that was faxed to them was a real business license of the particular country. I doubt they knew what "Vypis z obchodneho registra" that I faxed to them even meant. I believe that if I faxed them some famous Slovak novel, formatted to look like a business license and including the name and address of my company, they could not visually tell the difference and they probably do not employ Slovak language speakers to see the difference between prose from business licenses. I would love to be proven wrong.

Domain Ownership Control

While I did not try other authorities myself, I read about the process to issue certificates of several others. Some of them want you to prove ownership of a domain by telling you to create some file in the webspace of the server. They tell you to create for example http://yourdomain.com/sayhellotoourauthority/somerandomstring with some particular content. This is one of the better way to authenticate people who have control of a domain. However, it is quite funny to use this way because CA's, PKI, and TLS are here to protect communicating peers against known attacks to plaintext http. Seems weird that they themselves rely on this insecure way of communication to authenticate users. The attacks are well known - man in the middle attacks, DNS spoofing, etc. While this attack is certainly not the easiest one (the difficult part is getting access to the nameserver or to the physical link between CA and the authenticated domain), it is certainly not impossible. There are well established and tested tools to do this kind of attack.

The Solution?

Some CAs use a combination of these techniques. The best technique I have seen is the requirement to come to a local branch office of a CA, show your business license, ID card or passport, and driving license. The business license is checked with the court over the Internet. This also says who can act on behalf of a company. He is authenticated using an ID card, his presence is recorded on a tape, etc.

However, I believe that the current situation in Microsoft's browser is far from using this approach. I believe that MS Trust Root is built more on business contracts than on security standards. Microsoft and security. Sounds a bit stupid in one sentence.

I believe there should be some independent body (in the form of an organization like IANA and ICANN, but not controlled by the US government) which administers some common trust root. Certificates would be issued to CAs with the approval of local government organizations (in our country, it is the National Security Office which approves and disapproves the existence and operation of open CAs and accredited CAs). You could personally choose which countries' CAs you believe. All of the CAs should require a personal presence to authenticate and authorize the right to a certificate.

Also, the weak point in current implementations of x509 is that you cannot easily specify for which purpose you trust certain CAs. The purpose (web site authentication, S/MIME mail...) is on the certificate, but you cannot specify that you trust certain CAs for anything (for banking purposes) but another one only for freemail accounts and discussion boards authentication. It is not as easy in current web implementations anyway.

If you run a bank's web server, tell your users which CA you use (by postal mail) and tell them to always check the certificate. My bank does this (surprisingly), transferring all the liabilities to the user. (Someone robbed your account? You did not check the certificate? Oh, what a pity, it is your problem, not ours.) But if the bank recommends use of some particular user agent (usually MSIE) and does not tell users to delete all the "suspicious" CAs, they are liable for the client's money (and for the loss of it).

Maybe it is time to ask again: Whom do you trust? Do you trust Microsoft or AOL? Do you trust CAs they trust (for some reason, probably compensated by lots of money)? Being a well known CA does not guarantee it is a secure one.

System Profiling THROUGH RPC

by Screamer Chaotix

The Sun RPC (Remote Procedure Call) Portmapper running on port 111 can be your best friend - or your worst enemy. As usual it depends on what side of the fence you choose to play. For the purposes of this article, I will assume the reader is interested in exploring the possibilities of remote system profiling without the need for old fashioned programs such as finger.

Through the Portmapper running on 111, we can see what RPC programs are running on the remote machine, and may even get a chance to exploit one or two. The beauty of RPC is that, by its very nature, it's designed to be open to the Internet. And while most people have gotten around to getting rid of annoyances like finger, expn/vrfy on port 25, and of course, default accounts, not too many give RPC a second look. I could hypothesize as to why that is. Perhaps the most obvious reason being that port 111, by itself, is not really a security hole. Its best use, from an invader's perspective, is to show exactly what's running where. For brevity, we will focus on two RPC programs. One can be used to gain information about the target system, the other could potentially give us access to the machine. These daemons are rusersd and mountd. But first, how do we find them? You could take your target machine and simply run the client version of these commands against it to see if anything gives, but I prefer knowing if the RPC ports are up and running or not before I go attacking anything. To find open ports, a simple nmap scan will suffice:

```
screamer@localhost># nmap -sS -p 111
    192.168.2.* > port_111 &
```

I'll assume you have a machine and, for legality purposes, it's a comp you own (not Own). To see what RPC daemons are running, simply run the following command:

```
screamer@localhost># rpcinfo -p
    target.host.com
```

What will return is a listing of listening daemons, for example:

```
program     vers    proto    port
100007 1    udp     721      mountd
100025 1    udp     32790    rusersd
```

How convenient, we have both mountd and rusersd up and running. Let's begin by doing a little snooping. The first thing hackers would do a few years back was a quick and dirty "finger @target.host.com" to see who was logged into that machine. Nowadays, people know it's not a good idea to leave their login information lying around, even if it's just a username. What people don't realize however, is that they may still be giving out this very same information without realizing it. Enter rusers, which can be found through www.rpmfind.net if not already included in your distribution.

```
screamer@localhost># rusers -l
    target.host.com
```

For those of you wondering if that's a lowercase L or a one, it's the former (as in little lying larry). With this command, you will be brought back to the good old days of finger, as login information will appear before you (if people are logged in at that time of course). Here's an example for your viewing pleasure:

```
Login       Shell        Last Login
----------------------------------------------------------
screamer    /bin/bash    Wed Nov 2 from home.ctu.cia.gov
dash        /bin/bash    Thurs Dec 5 from grazer.ctu.cia.gov
```

Darn, and I thought by getting rid of finger I was safe! Guess not. So there we go, we have some login information. Now the next step I won't even get into. If you don't know what I'm talking about, it includes "password", "love", "sex", "secret", "god", last names, addresses, birthdays, spouse names, dog names, and maybe even a little social engineering.

Now let's move on to more important matters, shall we? Namely, mountd. Now mountd isn't all that terrible when properly configured (natch). The mountd protocol can be used to mount a remote drive onto a local one and allow you to view the contents of that drive as though it were on your local machine. In other words, you can see inside a computer without logging in. OK, let's use mountd to its full potential. To do this, we'll use a little program called showmount. The showmount client in a nutshell displays mountable drives on either your local or a remote machine. These are drives that can be mapped to a local drive and traversed as though that's exactly what they were.

```
screamer@localhost># showmount -e
    target.host.com
```

Which returns (if you're lucky):

```
/usr/bin               root
/home/johns            (everyone)
```

Great, so we have a couple of mountable drives there. The first is owned by root, which we can't touch. Fortunately, the next drive on the list looks like a user's home directory. Bingo! As Lord Nikon would say, you in the butterzone now baby. You can see inside this drive without even logging in! Begin by making a new directory to mount the remote one onto. In our case we'll call it new_mount. Then we mount the remote drive onto it, like so:

```
screamer@localhost># mkdir new_mount
screamer@localhost># mount
    target.host.com:/home/johns new_mount
```

If everything goes smoothly, you can now cd into your new_mount directory, type ls, and see everything inside that user's directory. Ooh, wow, you say. Who cares? I'm a hacker, I don't want to read someone's email, I want to explore the system they're using. Fortunately, with a home directory mounted on your computer you can. That, after all, is the magic of an .rhosts file. Yes that's right, rhosts, that file you should never have in your home directory is your ticket into this remote machine. Simply create an .rhosts file that contains this line.

```
your.machine.com  johns
```

From there, all you have to do is rlogin into the remote machine.

```
screamer@localhost># rlogin -l johns
    target.host.com
```

And there you have it. You're now logged into the remote machine as user johns. From here you can use any number of local exploits to achieve root. Naturally those all depend on the architecture of the machine, so look around or better yet try and figure out some things yourself (shocking concept, huh?). For just a minute, let's say you didn't find a mountable drive that belonged to a user but was however open to everyone. Possibilities exist for getting access here as well, potentially even as root. If you're lucky enough to find /usr/bin (or any other directory located in a user's path), you can mount the drive to your local machine and modify any number of programs in there to do your bidding. And if someone foolishly runs those programs as root (which is entirely possible), you can have some serious fun. Make ls discreetly add a new user with root privs, and voila, you have your very own backdoor. Try to be as inconspicuous as possible, name the new user "system_" or something to that effect, so it doesn't draw too much attention.

Last and certainly least, RPC is probably unnecessary on about 97 percent of the systems that use it. Why you need to show who's logged in through rusersd is beyond me, and why you would ever want to have people on the Internet mounting your drives on their local machines doesn't seem to make a lick of sense. These things do exist, believe me. Scan a university, you're bound to find a machine you can root with just a little effort. Naturally I can't actually recommend it, don't want to see anyone go to jail, but it's good to know what's possible, if only so you can better protect yourself. Until next time, break the system.

Thanks to everyone who helped, and shouts to the one and only Dash Interrupt, Unreal, w1nt3rmut3, dual_parallel, and pengs everywhere.

ROBOTS and Spiders

by StankDawg
StankDawg@hotmail.com

Everyone uses search engines. But did you ever wonder how they choose which pages to list and which pages to not list? You've all heard stories of private pages that got listed when they weren't supposed to have been. What stops these search engines from digging into your personal information? Well, without going into a lecture on why you should never store personal information on a publicly accessible website, let's talk about how search engines work.

The World Wide Web was named such because of the cliche that all of the pages are linked to each other like a spider's web. A search engine starts looking on a page and follows all of the links on that page until it gathers all of the information into its database. It then follows off-site links and goes on to do the same thing at all of the sites that are linked from that original site. This is really no different than a user sitting at home surfing the web except that it happens at an incredibly high speed. It is as though it were acting as an agent for the search engine. Due to its automation, it can quickly create and update its database. This automation is akin to a robot where it simply does the same repetitious job over and over. In this case, that job is to build a database of websites. Because of these reasons, the actual program or engine that does the work of crawling across the World Wide Web is called an "agent," a "spider," or, more commonly, a "robot."

"Isn't that a good thing?" Well, it can be. There are many good reasons for using robots. Obviously, it is very handy to have search engines to find things in the vast online world. It is even difficult to find documents on your own site sometimes! The use of robots is not only for going out and gathering up data, but they can be very personal and customized for your own site. One site can easily get into thousands and thousands of pages, sometimes more. It is very difficult to find and maintain documents on a site of this size. A robot can do that work for you. It can report broken links and help you fill in holes or errors on your sites.

"That's great, I want one!" Well, before you go jumping into something, think it through. There are also many drawbacks to using a spider. Firstly, you have to write the spider engine efficiently so as not to overload your server and also smart enough so that it does not start crawling on other people's sites and overloading their servers. If everyone had an agent out there crawling through everyone else's links, the web would slow to a grinding halt! The most important problem, however, is what I mentioned in the opening. Spiders will follow links to *everything* that it sees linked from another page. That means if you have a link to a personal e-mail, suddenly it isn't personal. Your company's financial documents may be on there somewhere. Did you have some naughty pictures that you took and only your husband or wife knew the link to? Can you say "oops?"

This raises a big concern over privacy, and rightfully so. Never put anything on the Internet that you don't want people to see. That is a general word of advice that you should follow regardless of spiders. You may have read stories about companies whose internal records are suddenly found floating around on the Internet. Blame hackers? Maybe you should blame robots and the administrators who do not know how to control them. All it takes is one site to start the robot and it begins to follow whatever links it is programmed to follow. Some employees may link to internal documents. Some databases may allow spiders to query from them. You never know who may be linking to what, and by not having a well designed web site, you may have just taken your top secret project and shared it with the world.

So you see, there are some good things and some bad things. Luckily, there are ways that you can control robots and hopefully limit the bad things. There is a standard called the "robots.txt" exclusion file. It is a simple ASCII text file that allows you to tell any robot visiting your site what they can and cannot access. Here is a sample file:

```
#
# robots.txt file for http://www.StankDawg.com/
#
# last updated: 09/06/2003 by: StankDawg
#
# WTF R U Doing here?  R U A ROBOT?
# R U A SPIDER?  R U 31337?
#

User-agent: *
Disallow: /incoming/
Disallow: /downloads/
Disallow: /webstat/
Disallow: /pub/

User-agent: Hackers-go-away
Disallow: /T0pS3cr3t/

User-agent: They-will-never-find-this-one
Disallow: /h1dd3n/
```

You will notice that there are comments (starting with the "#" sign) and two other important fields. Proper use of these fields can limit most search engines and spiders that honor the exclusion file.

The first field is called the "User-agent" string. Each program visiting your website, human or otherwise, is using a piece of software. For humans, it is called a web browser like Mozilla, Firebird, Konqueror, or dozens of others. The name of this agent is sent with every page request. If you look at raw log files from your web server, you can see who visited your site and what agent they used. The majority of them will be Internet Explorer since most surfers are using the Windows operating system. You can look at your logs and find some interesting types of clients out there. Well, since robots are programs too, they also have an agent string. In the robots.txt file (which must reside in the root directory of your web server home) you can single out any agent to block it.

The second field is the actual file or directory that you do not want accessed. The field name you would use is "Disallow". Both the "User-agent" and the "Disallow" must be followed by a ":" and then the data that specifies what you want done. If you want to stop the agent called "googlebot" from accessing the file called "privatestuff.html" you would code the following lines:

```
# This is a comment above the sample code.
#
User-agent: googlebot
Disallow: privatestuff.html
Disallow: /images/mysexypics/
```

As you can see, the syntax is very simple. What you need to do is think about which things you want kept hidden from which agents. If you want to hide several different files or directories, you would use multiple "Disallow" lines. In the example above, I also block access to the entire directory called "/images/mysexypics/" which could have been very embarrassing! Be careful to realize that this only blocks *one agent!* Usually people do not distinguish one agent from another in practical application. If something is to be kept hidden, it should be hidden from all agents, not just "googlebot" as in the example above. One way of doing this is to use multiple "User-agent" strings. This is never complete and there are always new spiders coming out that would not be on your list unless you constantly update it. The better way to do this is to simply use a wildcard of "*" which tells *all agents* to follow the subsequent "Disallow" commands. Along the same lines, you can also tell robots to ignore your entire site by using the "Disallow" string of "/" which will stop the robot from looking at anything! (Note that you cannot use a "*" wildcard in the Disallow field; you must specify a path.)

```
# This is a global "stop all robots" example
#
# Note that comments can be put anywhere
# on a line, and not just above the fields.
# They can come after the string.
#
User-agent: * # This string stops ALL robots
from going into...
Disallow: / # ANY of the directories
```

An alternative to using the robots.txt file is to use special "meta" tags in your HTML. Some people may not be able to create a robots.txt file for one reason or another. You can also add a meta tag in the HTML of every page that you code. The meta tag name is simply "robots". This meta tag will allow or disallow robots by using keywords in the meta tag such as "all" to allow it to be included in the search engine or "none" to stop it from being added to a search engine. There are other options as well, but these should suffice for most users.

Now here is the catch. (There is always a catch.) The keyword is "honor" which I mentioned earlier. While most commercial search engines will currently honor your robots.txt file, it is not a requirement that they do. It is an optional standard that is not enforced by any agency. That's right, it's on the honor system. I am sure that there will come a day when the search engine competition will become so fierce that the engines will begin to index all pages regardless of exclusion requests so that they will gain an "advantage" over other search engines. Also, you have to realize that anyone can write a spider or a robot! Since it is optional whether or not they honor your exclusion requests, they may still waltz right through your site and ignore all of your "do not enter" signs. This is the reason that I mentioned earlier that you should never, *ever* put really personal, private, or valuable information in a publicly accessible location.

Finally, you should also realize that just because these are intended for robots (or programs) to look at, that doesn't mean that humans cannot look at them as well. I have found many, *many* backdoors and "hidden" entrances simply by looking at a site's robots.txt file. You have full permission to poke around my robots.txt files and maybe you will find some interesting super secret 31337 stuff!

Further Reading

http://www.robotstxt.org/
http://www.searchengineworld.com/robots/robots_tutorial.htm

Shoutz: As always... my home-dawgs in the DDP, Zearle, Saitou, people who are willing to read and learn, whoever invented the new Reese's "big cup," and people who try to use robots.txt files as a substitute for security.

Living Without an SSN

by Lucky225

In mid November of 1936 when the first social security numbers were issued, they were never meant to be thought of as a form of identification. Today however every major corporation in the U.S. requests this number from consumers for identification and to run credit checks, or so they claim. Utility companies including gas, electric, telephone, and cable TV companies all request this information as well as your bank, your credit card issuers, and pretty much anyone else you can think of. You might assume there is some law or statute that requires these corporations to obtain this information before providing you with their services. However there is generally no statute provided that requires these companies to obtain that information for any reason.

With identity theft becoming the fastest growing crime in this country, one in 20 consumers was a victim of credit card theft last year. It is predicted that about 750,000 people a year may become victims of identity theft. Most corporations insist that they require a social security number to validate who you are. However, if you look at it from a different angle, you might notice that this requirement is exactly what makes identity theft so easy. Think about it. Utility services, bank and credit card accounts, cell phone activations - all this can be done over the phone or the Internet needing only a person's name and social security number and some other easy-to-find information like a birthday. All of this is done without providing any photo identification at all and it can be done completely anonymously using P.O. boxes or private mailboxes. With that said, think about all the places you've given your social security number to. Think about all the computer databases holding that information right now. Think about the fact that there may be an untrustworthy employee at TransUnion staring at your credit report with your information on it right now and you'd have no way of knowing.

To give a prime example of this, let me tell you about a story that happened with my mom. One day she decided to buy a cell phone from a kiosk inside Sam's Club. The kiosk was for Verizon Wireless. Two years passed by and we received a notice from Cingular Wireless about unpaid cellular service, even though we have never had any cell phones with Cingular Wireless. After an investigation, it was determined that the cell phone was activated the same day she had signed up for her cell phone with Verizon. It is unclear who set up the cellular service, but anyone who was able to take a glance at the paper application that had my mom's SSN on it could have quickly written that information down and then set up service in her name.

Keeping all of this in mind I have recently become a privacy advocate. The Office of Privacy Protection in California has declared that the SSN is a unique privacy risk because no other identifier plays such a significant role in linking records containing sensitive information that individuals generally wish to keep confidential. Because the SSN is such a privacy risk, I do not reveal it to any portion of the private sector. By not giving out your SSN you can actually help prevent identity theft because most companies will require you to show picture identification and other material if you do not supply an SSN ensuring that you are the person you claim to be. And because no SSN is ever recorded by the company, anyone who looks at your account information on the company's customer database will not be able to use your information to obtain credit or services in your name. Luckily I live in California where the CPUC has ruled that all utility companies (excluding cellular unfortunately) cannot deny you service simply for lack of an SSN or for refusing to provide it. But the utility company may require a deposit if you do not supply this information. You will get the deposit back however.

By making it a policy not to provide your SSN to any private organization, you will come across some things that may not be convenient for you. Since I have started this policy no utility company has ever obtained my SSN. But when it comes to credit, everyone wants your SSN. I had a bank account for about a year when they offered me an unsecured credit card. I figured I'd apply for it but leave my SSN off the application. About a month later I got the credit card. It informed me that I had to call from my "home phone number" to activate the card. I forgot which phone number I had written on the application so I called customer service on the back of the card to ask them. The representative informed me that it was not necessary to call from my home phone number, that she could activate the card over the phone. All I had to do was verify my social security number. I told her that the only reason I applied for credit was because the person at my bank's branch let me apply without writing in my SSN. She informed me that the SSN had been retrieved through the application process from my bank account information. I said that I had not consented to this and that I would not activate the card unless the social security number was removed from the account. She actually agreed to remove it for me after verifying some other information and adding a password to the account. I then went to the bank and closed my checking account.

I have since been using a stored value card that does not require you to provide a social security number. My paycheck is direct deposited on to the card and it works just like a check card. You can receive a similar card by going to www.cardenroll.com (claims to require SSN now - just enter 000-00-0000). There are other cards out there that allow you to add funds from Western Union or MoneyGram locations for a fee. Some of the stored value cards ask for an SSN but do not verify it. Anyhow, the downside to stored value cards is that there is no way to deposit a *check* into the account. I recently received a check from my insurance company for about $2800 issued from Bank Of America. It took me three Bank Of America's and talking to several branch managers before I found one who would cash my check for me. The other two branches told me the check was "over their limit" for non-customers. I advise you to try local bank branches for opening up checking accounts without SSN.

The thing that bugs me is there is no law requiring a bank to obtain an SSN for non-interest bearing checking accounts. There is no interest being accrued, thus they don't have to report to the IRS. My bank won't even open an account for me using two forms of ID, one of which is the credit card issued by their bank!

Also hard to deal with are credit bureaus. Once they have your SSN, it's pretty much there for life. However I did manage to social engineer TransUnion into removing my SSN, claiming the one on file was inaccurate. Under the Fair Credit and Reporting Act, they are required by law to remove inaccurate information. They agreed to remove it "temporarily" as my SSN would be reported to them by my creditors, they claimed. Little did they know my creditors didn't know my SSN and so I now have credit and a credit report with no SSN attached to it!

As I mentioned, the California CPUC does not regulate utilities so it is difficult to obtain a cell phone without an SSN because almost every carrier requires this information to "run a credit check" - or so they claim. I did however convince an AT&T Wireless salesperson to run my credit using the SSN 000-00-0000 and I got approved - and the inquiry showed up on my TransUnion report. So it is possible to get a cell phone through AT&T Wireless without an SSN, though it may be hard to convince the salesperson that they don't need your SSN to run credit.

The best approach when applying for credit or services is to claim you do not have an SSN. If you want, move to Oregon and get a driver's license there. They don't even require an SSN for a driver's license or identification card! Carry around your Oregon license and claim you have never applied for a social security card because there is no law requiring you to do so. I carry around a copy of my TransUnion credit report showing there is no SSN and a letter from my bank stating there is no social security number on my credit card account and it usually helps assist me when I apply for services or credit at places that claim to require a social security number. It's fun to see people's reactions when I tell them I'm a privacy advocate and do not give out my social security number and then hand them my TransUnion credit report along with the letter stating there is no SSN on my credit card.

Helpful Links

http://www.civil-liberties.com/soc_security/forms/bank_not.pdf - notice to banks regarding use of SSN.

http://www.cardenroll.com - stored value card.

http://www.privacyrights.org - privacy info.

http://www.privacy.ca.gov - privacy laws in California

More Fun With Wireless Hacking

by VileSYN

As the prices go down, wireless becomes more and more common. While many people ignore the vulnerabilities that WiFi holds, it's an easy way for anyone to enter the network. Even setting WEP keys will not keep a determined hacker from compromising the WiFi AP (access point) or router.

Many tools are available for various operating systems to do such tasks. NetStumbler for Windows, MacStumbler for MacOS, Wellenreiter for Linux, and BSD-Airtools for Free/Open/NetBSD are WiFi network stumblers to help find APs. Most of these applications can use a GPS to map the access points detected while scanning. Such stumbling tools are what make wireless hacking such a threat. Using these tools is quite simple and straight to the point. Each will detect the APs from stray signals, detect WEP transmissions, channel, signal strength, and MAC address. While they also determine the manufacturer by the MAC address, some entries can be incorrectly identified.

A way of finding the exact manufacturer by MAC address can be seen on the page http://standards.ieee.org/regauth/oui/oui.txt. Every MAC address and manufacturer is listed. This brings us to another key to entering the network. Sometimes you can enter the network easily by using DHCP, but not all networks have DHCP available. In such a case, there are a few ways to obtain the address of the AP.

The first way to acquire the IP is to use the default IP that the wireless device is set to. For instance, D-Link routers use 192.168.0.1, and their access points use 192.168.0.50. On the other hand, Linksys uses 192.168.1.1 and Netgear uses 192.168.0.1. If the default IP is not the IP of the AP, then you can use a sniffing utility to capture packets coming from WiFi signal.

Once you have gained the IP and enabled an associated connection to the AP, it's time to connect elsewhere. Even though you might have a connection, WEP might be holding you back. WEP is an encryption used for wireless networking stated in the IEEE standard for 802.11a/b. When they made this standard, they did not think of what could be done to crack it. Every minute a small amount of WEP broadcasts are sent over the network. Each broadcast frame is the same, allowing these frames to be captured easily and decrypted without worrying about the packet changing. With WEP tools like WEPCrack, AirSnort, and BSD-Airtools' Dweputils, cracking a WEP dump can be accomplished within a few minutes. Some 104-bit (128-bit) keys can take up to 36 hours depending on the speed of your system, but logging your hits or using a GPS can show you where that network was when you first found it so that you can go back after breaking the key.

Once this is all done, the network is under your control. From here you don't have to worry about the router blocking your system from anything and sometimes receiving an SNMP log or two. If you know the default password for the specific AP, you can always go for that first off. If you do not know the defaults for WiFi devices, go to the manufacturer site and look up models to find the documents with the defaults.

Another way is to use a terminal service like Remote Desktop for Windows or rdesktop for Linux/UNIX to connect to a Windows desktop. (Remember, most people do not set a password for the Admin or Administrator account in Windows.) From there you can use the local browser and see if any cookies were used in the past to log into the AP.

Remember, even though you're taking a backdoor into the network, logs can still show your existence. Clearing router logs or entering the network with a MiTM (Man-in-The-Middle) attack or spoofed MAC will look like normal activity on the network. Providing a backdoor from the router and placing a route to a service on another system to get in can do a vast amount of good for your final compromise.

These particular methods are slowly becoming obsolete. WiFi Protected Access (WPA) provides better authentication and stops the repeating frame encryption packets. Many wireless devices are now starting to have the option of disabling signal broadcasting and disallowing signals to be "stumbled" upon. Even though this new technology is being offered, it doesn't mean the weak link in any network is becoming smarter or that people are even upgrading. Rather, if you plan to secure your WiFi network or conquer another, signals will always be monitored.

Thanx to: The error between the chair and the computer, FBSDHN, SE, and all those other people.

WEP: Not For Me

by 0x20Cowboy

I know a thing or two about wireless networking and security and therefore I assume everyone else does too. But nothing could be further from the truth. In fact, what I found out yesterday is pretty scary.

I recently received a contract to port some applications to the Pocket PC handheld computer. One of the bonuses was that I received a free Pocket PC and, since the application I am working on requires networking, I also got a spanking new Netgear 802.11b MA701 wireless network card (very cool card - I highly recommend it).

These handheld computers are pretty powerful beasts. The one I was given has a 400mhz processor and 64mb of internal memory. That's a pretty good box even for a desktop (I didn't say it would run Half Life, I said it was pretty good) and you can add lots of external items - USB, monitors, keyboards, etc.

The networking is pretty amazing as well. One of the features of the networking card's software is an AP (Access Point) browser which shows you all the available networks in your general vicinity (much like the one on the Windows(r)(tm)(sm) desktop). When I first hooked up the wireless card, I started to connect to my access point when suddenly I saw three other networks - two without WEP enabled.

"Um... that's odd. Those guys should be more careful," I thought and wrote it off as rare.

Later that evening, my girlfriend wanted to take me to a play (yuck). I talked her into letting me take my new PDA with me, and I scanned for APs on the way to the play (she drove).

Jesus Christ, they were everywhere. I mean everywhere. Every time I hit "scan" I would get four or five in the list. Seventy percent of them did not have WEP enabled and most had the default SSID.

We stopped at a rather long stop light and one SSID said "linksys." I own a Linksys and I remembered the default setup so... wtf... I clicked "join." DHCP gave me an IP, I browsed to 192.168.1.1, a dialog popped up, I typed "admin" as the password, and two seconds later I was looking at the router configuration. Not only did I have an Internet connection, I 0wn3d the AP - all while waiting for the light to change.

Depending on how you choose to live, this is either a great and wonderful playground or an absolute nightmare. One could, potentially, just drive around and remain rather anonymous. Not only changing IPs, but changing physical locations, and with the added bonus of a really really small computer you could probably just walk around with and no one would notice it. How hard would it be to track someone bouncing off a couple of servers *and* changing where they are plugging in from?

When I got home I did a bit of research on wireless routers and I compiled a list of popular APs and their default settings (see list below). Wireless network router makers need to at least enable WEP by default, the setup utilities need to help Joe Shmoe turn it on, or common users are going to get pimped hard when wireless toys become cheaper.

Here are the default settings for common APs. Anything listed as NULL is something I couldn't find. Often, when connecting to an AP, it will tell you the model in the password dialog box.

ssid	manufname	model	address	uname	password
NULL	Netgear	MR814 (v2)	192.168.0.1		password
NULL	Netgear	WGR614	192.168.0.1		password
NULL	Netgear	WGT624	192.168.0.1		password
NULL	Netgear	WG602 (v2)	192.168.0.227		password
NULL	Netgear	ME103	192.168.0.224		password
NULL	D-Link	DI-624 (a,b&c)	192.168.0.1		admin
NULL	D-Link	DWL-2000AP	192.168.0.50		admin
NULL	D-Link	DI-774	192.168.0.1		admin
NULL	D-Link	DWL-1700AP	192.168.0.50:2000	admin	root
NULL	D-Link	DWL-1000AP+	192.168.0.50	NULL	NULL
NULL	D-Link	DWL-700AP	192.168.0.50	admin	
NULL	D-Link	DI-754	192.168.0.1	Admin	
NULL	D-Link	DI-764	192.168.0.1	Admin	
NULL	D-Link	DWL-6000AP	192.168.0.50	Admin	
NULL	D-Link	DWL-5000AP	192.168.0.50	Admin	
NULL	Actiontec	R3010UW	192.168.0.1	admin	
NULL	Actiontec	AU802C	192.168.1.240	Admin	Admin
linksys	Linksys	WAP54G	192.168.1.245		admin
linksys-a	Linksys	WAP55AG	192.168.1.246		admin
linksys	Linksys	WRT54G	192.168.1.1		admin
linksys-g	Linksys	WRT55AG	192.168.1.1		admin
linksys	Linksys	WRV546	192.168.1.1	admin	admin
linksys	Linksys	BEFW11S4	192.168.1.1		admin
linksys	Linksys	WAP11	192.168.1.251		admin
linksys	Linksys	WAP51AB	192.168.1.250		admin
linksys	Linksys	WAP54A	192.168.1.252		admin
linksys	Linksys	WRT51AB	192.168.1.1		admin

War Driving with a Pocket PC

by RaT_HaCk
RaT_HaCk@net-troy.com

War driving has become another great American pastime. It has been given many names, and a great many different tutorials have been written on this subject. But there has been one aspect that has failed to get any attention even with all its possibilities and this is war driving with a Pocket PC. A Pocket PC is the perfect tool for war driving since it is easily hidden and the user can look relatively harmless while tapping away at the screen.

WiFi Cards

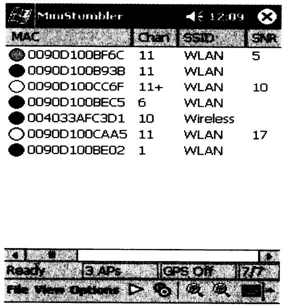
Many Pocket PC's are coming out with integrated WiFi cards. But for those that don't have integrated WiFi cards, you need to acquire one. There is a great variety out there from which to choose. Among the choices are Secure Digital cards that come with built in storage space, slim Compact flash cards, and the classic PCMCIA type cards. Many Pocket PC's, however, do not come with the luxury of having a PCMCIA. Even though there is a Compact flash to PCMCIA converter, it is bulky and impractical. So most users are reduced to the Secure Digital cards and the more prominent Compact flash cards.

Access Point Sniffing

In order to find access points you can connect to, access point sniffing is necessary. Essentially, access points are computers or other devices that serve as a point which you can connect to via wireless. There are many types of programs out there that enable you to do this. Here are just a few of the more noted ones available for Pocket PC use:

Mini Stumbler: http://www.netstumbler.com

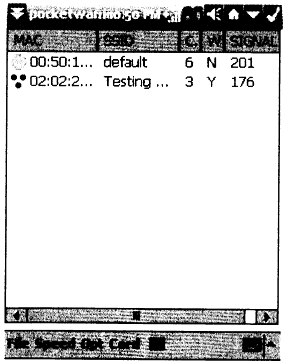
Mini Stumbler is the Pocket PC counterpart to the famous Stumbler program called Net Stumbler. This program is a great war driving tool because it is very fast and reliable for finding access points. If you have a GPS card on your Pocket PC, it maps the AP's location. It will even inform you of the exact longitude and latitude of your position standing from the AP.



```
MAC            Chan  SSID      SNR
● 0090D100BF6C  11    WLAN      5
● 0090D100B93B  11    WLAN
○ 0090D100CC6F  11+   WLAN      10
● 0090D100BEC5  6     WLAN
● 004033AFC3D1  10    Wireless
○ 0090D100CAA5  11    WLAN      17
● 0090D100BE02  1     WLAN
```

Pocket Warrior: http://www.pocketwarrior.org

Pocket Warrior is almost identical to Mini Stumbler with the exception that it supports Prism cards and some Orinoco cards compared to Mini Stumbler which only supports Orinoco cards. However, some Prism cards' drivers may not be supported. So I suggest downloading the Intersil Reference Driver available courtesy of Net-Troy: http://www.net-troy.com/drivers.



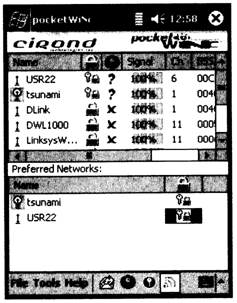
```
MAC          SSID       C  W  SIGNAL
00:50:1...   default    6  N  201
02:02:2...   Testing ...  3  Y  176
```

PocketWinc: http://www.cirond.com

PocketWinc is not the fastest scanner but it can connect to AP's quickly. It also automatically detects if there is an Internet connection present in the access point as well as if there is a WEP key configuration. PocketWinc also provides multiple network diagnostic tools.

Packet Sniffing

Packet sniffing is basically taping all traffic that goes through your target network and this is very useful in war driving. You can discover many interesting things by sniffing people's traffic passwords, WEP keys, private conversations, and much more. AirScanner is a great Pocket PC sniffer program. It has the ability to sniff many different varieties of packets and can easily pick up something useful. It is also possible to filter the type of packets which you are sniffing, thus narrowing the search for what you're trying to pick up. Another great feature is the ability to save your sniffed sessions in ethereal format and load it on your PC for further analyzing. AirScanner is available at: http://www.airscanner.com.



Name			Signal	Ch	BSS
USR22		?	100%	6	00C
tsunami		?	100%	1	004
DLink		x	100%	1	004
DWL1000		x	100%	11	000
LinksysW...		x	100%	11	000

Preferred Networks:

Name
tsunami
USR22

Network Diagnostic Tools

At some point in your war driving outing you're going to need to test the network - for example, to check the speed to see if the connection is alive, what ports are open, and, most importantly, to learn more information about it. This is why network diagnostic tools are very useful in war driving. VxUtil is a great set of network diagnostic tools that comes with a port scanner, traceroute, whois, time service, DNS lookup, and many more. This program is available at http://www.cam.com. This site also contains lots of other software that will aid your Pocket PC experience, but unfortunately most of the other programs will cost you.

Mapping Drives

Another interesting thing to do when you are connected to someone's computer via WiFi is to map their drives to your Pocket PC. This can be very productive. There are various way to accomplish this, but the easiest way I have found is with a program called Resco Explorer available on http://www.resco-net.com. This program isn't freeware, but it is worth the money. With just a few taps on your Pocket PC screen, you will be able to see everything on your subject computer.

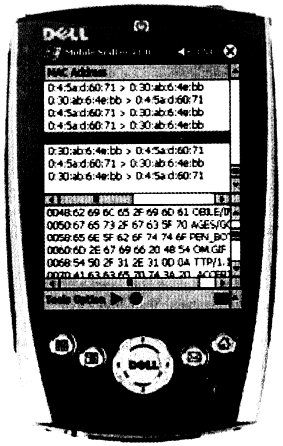
Hitting the Streets

With whatever setup you have put together with your Pocket PC, walk, drive, or take a bus and turn on the AP scanner you have chosen and let it pick up access points. When you discover an access point that piques your interest, connect to it manually if you are not using a tool that will automatically connect you. Then feel free to explore your target computer with your sniffer, network diagnostic tools, or just surf the Internet and so on.

End Thought

I hope this has opened up your eyes about the many possibilities that war driving with a Pocket PC offers. Even though it may not be as powerful as the ever-so-popular laptop, in some situations trading in that excess power for something stealthy, compact, and easily hidden may be preferred. Have fun....

Shout outs to: Rasem, TeraPhex, Moogleeater, Vfuller, A7hena, Poru.



```
0:4:5a:d:60:71 > 0:30:ab:6:4e:bb
0:30:ab:6:4e:bb > 0:4:5a:d:60:71
0:4:5a:d:60:71 > 0:30:ab:6:4e:bb
0:4:5a:d:60:71 > 0:30:ab:6:4e:bb

0:30:ab:6:4e:bb > 0:4:5a:d:60:71
0:4:5a:d:60:71 > 0:30:ab:6:4e:bb
0:30:ab:6:4e:bb > 0:4:5a:d:60:71

0048:62 69 6C 65 2F 69 6D 61 CBLE/I
0050:67 65 73 2F 67 63 5F 70 AGES/G
0058:65 6E 5F 62 6F 74 74 6F PEN_BO
0060:6D 2E 67 69 66 20 48 54 OM.GIF
0068:54 50 2F 31 2E 31 0D 0A TTP/1.
```

Verizon's Call Intercept

by decoder
decoder@oldskoolphreak.com

Call Intercept is a service offered by Verizon which prevents callers that do not send any Caller ID information from directly ringing your line. Instead, callers hear a recorded announcement informing them that you subscribe to this service, then they are prompted to record their name for identification. If the caller does not record their name, then your phone does not ring. If they choose to record their name, your phone rings with a distinctive pattern, and you have the choice of either accepting or denying the call through an automated menu. The monthly charge for this service is $6.00, although it is included in some of Verizon's premium plans.

While this service does have some flaws, I feel that it is better than Anonymous Call Rejection (ACR) for certain types of annoyance calls. For instance, telemarketers can still get through to a line equipped with ACR without sending any Caller ID information. There are also some PICC's (Pre-subscribed Interexchange Carrier Codes, commonly referred to as 10-10 numbers) that can be used to bypass ACR. The reason for this is that ACR is meant to reject callers who block their number by using *67. However if an ANI-F(ail) occurs, the Caller ID information is missing and the call goes through just fine. The display will show "out of area" and no phone number will appear. Keep in mind that *67 sends a Caller ID signal of its own, while a flex-ANI fail will cause the absence of any Caller ID information, due to the fact that Caller ID information is derived from the flex-ANI. Call Intercept will not let *any* calls directly ring your line unless a number appears on the Caller ID display. ACR is designed to reject certain types of calls and let everything else through. Call Intercept is designed to accept only certain types of calls, and reject everything else.

How It Works

When Call Intercept is activated, anonymous callers trying to reach you will hear an announcement explaining what Call Intercept is. Then they will be prompted to record their name. They can also enter a four digit override code to bypass Call Intercept (more on this later). At this point your phone will ring with a distinctive pattern and your Caller ID display will notify you that it is a Call Intercept call. During this time, and until you decide how to handle the call, the caller will hear hold music. When you pick up the phone you will hear, "Someone is waiting to speak with you. For more information, press 1." You will then hear the caller's name as they have recorded it and you will have the options of accepting the call, denying the call, playing a "sales call refusal" to the caller, or sending the call to your Home Voice Mail, if you subscribe to it. The "sales call refusal" is pretty useful. If the caller is stupid enough to identify that they are a telemarketer, you can have this announcement played to them. It will inform the caller that you do not accept telephone solicitations and wish to be placed on their Do Not Call list. I have never had a telemarketer attempt to ring my line through Call Intercept, although with the new National Do Not Call List, some of these phone solicitors may become desperate.

I should note that Call Intercept may not interact well with certain Verizon services as well as some types of phone calls. You cannot have Anonymous Call Rejection active on your line with Call Intercept. I suppose the reason for this is that ACR would override Call Intercept, and all anonymous calls would get sent to the ACR intercept message. ("We're sorry, the person you are calling does not wish to speak with callers that block delivery of their telephone number" or something like that depending on where you live.) Also, you cannot use *57 to trace calls that came in through Call Intercept. Remember, *57 is a customer originated trace, and when you receive a call through Call Intercept, it is effectively a call transfer. International cellular calls as well as collect calls made without the assistance of a live operator may also experience difficulty completing calls to your line.

My Experiences

When I first subscribed to Call Intercept, I was asked to choose a four digit bypass code while on the phone with the customer service representative. This is the code that you would give to anyone whom you wished to have the ability to bypass your Call Intercept service. Upon hearing the Call Intercept greeting, an authorized caller would enter the code, and then would be able to directly ring your line, without sending any Caller ID transmission. The Caller ID display would read "Priority Caller," accompanied by the distinctive ring.

According to the Verizon Residence Services User Guide, in former GTE states the subscriber would be able to access their Call Intercept service by calling a toll-free number. Instead of choosing a bypass code while on the phone with the customer service representative, as is done in former Bell Atlantic states such as my home state of New York, customers in the former GTE regions would have their bypass code defaulted to the last four digits of their home telephone number. When they called the toll-free number, they would be able to change the bypass code, as well as turn Call Intercept on and off. This number was not published in the User Guide.

In the past, when someone would try to ring my line through Call Intercept, my Caller ID display would read "Call Intercept" in the name field and the phone number would come up as my area code followed by all ones. This was the case until recently, when the display began showing a toll-free number. It now displayed 800-527-7070 as the Call Intercept number. This is the number used in former GTE states for a service known as Call Gate. Basically, Call Gate lets you control your phone line in various ways. You can "blacklist" and "whitelist" certain incoming and outgoing numbers. You can block or unblock international calls and calls to premium (900) numbers. You can even block *all* incoming or outgoing calls. It pretty much gives you complete control of your dial-tone. These features, along with Call Intercept, are what Verizon refers to as "Advanced Services."

When you call 1-800-527-7070, it informs you that you have reached Verizon's Advanced Services, and you are asked to enter your home telephone number. I recall attempting to call this number in the past, but it wouldn't accept my phone number because this service isn't available in my state. After seeing this number appear on my Caller ID display as the Call Intercept number, I tried calling again. When I entered my home telephone number this time, it accepted it. I was asked for my PIN which is, of course by default, the last four digits of my phone number. From here I was able to hear or change my bypass code, as well as turn Call Intercept on or off. Verizon never informed me that I was able to use this service, and when I first signed up with Verizon, it wouldn't work for me. Apparently this number is now being used in the former Bell Atlantic states to control the Call Intercept feature.

Hacking It

This is where the security issue comes into play. You can call this toll-free number and enter in anyone's phone number in New York State who subscribes to Call Intercept. The PIN will be the default every time. The reason no one has changed their PIN is because Verizon has yet to inform anyone of this service. Anyone who subscribes to Call Intercept in New York is vulnerable. You simply dial 1-800-527-7070, and when prompted, enter the telephone number of someone in New York who subscribes to Call Intercept. When it asks for the PIN, enter the last four digits of their telephone number and you're in. From this menu you could listen to their bypass code, change it, change the PIN for the toll-free number, or turn off Call Intercept altogether. The service that they think is protecting them from unwanted and annoyance calls can actually facilitate these types of calls because of a security hole.

There is an easy solution to this security hole. Require ANI verification in order to initialize the service. It is a common practice for other services such as remote call forwarding. As a matter of fact, Verizon does require that the initialization be done from the line which subscribes to Call Intercept in every other former Bell Atlantic state except New York. If you were to call the toll-free number and enter a Call Intercept subscriber's phone number in Vermont, Massachusetts, New Jersey, etc., you will be informed that the service must be initialized from the telephone number which subscribes to the service. Once the initialization is complete, you may access your services from any telephone. It is quite obvious that Verizon's customers in those states are also unaware of the toll-free number to control their service because they haven't initialized it yet. Fortunately, ANI verification is used so they are not left vulnerable. Why New York does not require ANI verification is unknown to me, but what I do know is that *anyone* was able to administrate my Call Intercept, and I would have never known.

Conclusion

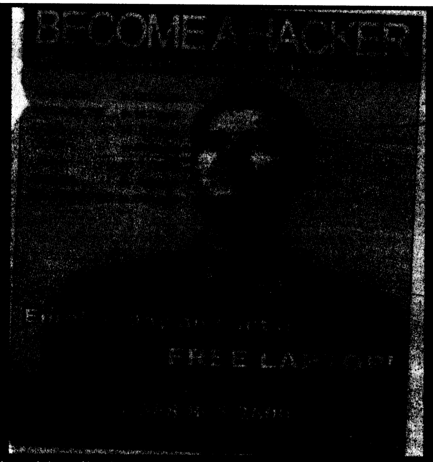
Hopefully, Verizon will rectify this situation because it simply does not make sense to require ANI verification everywhere except New York. You could always spoof the ANI, or beige box from the customer's line if you are determined to access someone's Call Intercept, but in New York, you simply need to call a toll-free number from anywhere you wish and enter a default PIN code. Now you have control over their acceptance of anonymous calls.

Other than being a large security issue in New York, Call Intercept is a great service. By subscribing to it, you will receive close to zero telemarketing calls. Having your anonymous callers hear hold music while you decide how to handle the call is pretty nifty as well. I have honestly enjoyed having this service and would highly recommend it to all Verizon customers. Just remember, if you are considering subscribing to Call Intercept, or if you already have it, call 1-800-527-7070 and change your PIN! Especially if you live in New York, unless I already have!

Useful Verizon Numbers

1-800-527-7070 Call Gate (use for Call intercept in Bell Atlantic states)
1-800-870-0000 Call if you misplace your PIN
1-800-275-2355 Verizon Repair
1-800-518-5507 Verizon Unlawful Call center
1-800-254-5959 Verizon Unlawful Call center (TTY)
1-877-TRACE-4U Call Trace Information line
1-800-257-2969 Call Trace line (for GTE states)
1-800-562-5588 to test All Call Blocking (in PA only)
1-NPA-890-1900 to test All Call Blocking (in NY & CT only)
1-888-599-2927 to test All Call Blocking (in New England)
1-888-294-1618 to initialize Ultra Forward service (call from ANI)
1-800-284-1687 to initialize Ultra Forward service (in MA & NY)
1-800-414-9898 to use Ultra Forward (in NY, CT, MA, ME, VT, NH & RI)
1-212-338-8300 to use Ultra Forward (from anywhere else)
1-800-483-1000 Customer Service (in PA & VA)
1-800-234-2340 Verizon's Customer Information line

Shouts: Lucky225, accident, Licutis, NotTheory, w1nt3rmut3, icOn, Captain B, Majestic, Scott, doug, phractal, Scr00, WhiteSword, RijilV, Eta, parano|a, dual_parallel, bland_inquisitor at Radio Freek America, Slipmode at www.slipnet.org, and StankDawg at www.binrev.com.



Yes, this is what it's all about. All you have to do is pay these guys thousands of dollars and you too can look proudly into the distance and ponder on what you will do with your newly purchased hacker prowess. Nice phone number too, fellas.

And in the year 1997, for two days and nights, Beyond HOPE infested the City.

Fun With [redacted]

by methodic
methodic@libpcap.net

Hping is a very powerful tool that lets you create arbitrary packets with all types of options, as well as show the output of any returned traffic from the host you're hpinging. By default when you hping a host, it will send UDP packets to the host's port 0. As you will see later on, you can change this behavior by specifying a source port, a destination port, a different protocol, the list goes on. You'll find that most of hping's output deals with low-level information from the packets received, which is beyond the scope of this article. For now, we'll only be interested in a few select things.

Let's start off by running a plain hping against www.2600.com to get our bearings on hping output:

```
[root@clotch root]# hping2 -c 3 www.2600.com
HPING www.2600.com (eth0 207.99.30.226): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=207.99.30.226 ttl=49 id=85 sport=0 flags=RA seq=0 win=0 rtt=50.9 ms
len=46 ip=207.99.30.226 ttl=49 id=48918 sport=0 flags=RA seq=1 win=0 rtt=51.0 ms
len=46 ip=207.99.30.226 ttl=49 id=19729 sport=0 flags=RA seq=2 win=0 rtt=50.4 ms

--- www.2600.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 50.4/50.7/51.0 ms
```

As you can see, we are able to find out some pretty interesting stuff. (If you want to see even more, enable verbose output with the -V flag.) We know that the remote host uses random IP ID's, which means they aren't as vulnerable to information gathering and spoofing attacks. Also note the flag that came back: RA. The A stands for ACK, meaning "I acknowledge your request," and the R stands for RST, meaning "Resetting connection. Good-bye."

Next, we'll see what kind of ICMP requests www.2600.com responds to. In hping, you enable ICMP packets with the -1 flag. By default, hping will send ICMP echo-request packets (ICMP Type 8, standard ping):

```
[root@clotch root]# hping2 -1 -c 3 www.2600.com
HPING www.2600.com (eth0 207.99.30.226): icmp mode set, 28 headers + 0 data bytes
ICMP Packet filtered from ip=207.99.30.226 name=UNKNOWN
ICMP Packet filtered from ip=207.99.30.226 name=UNKNOWN
ICMP Packet filtered from ip=207.99.30.226 name=UNKNOWN

--- www.2600.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

So we know that www.2600.com is blocking ICMP echo requests. We could also check to see if www.2600.com answers to other types of ICMP requests like address mask or timestamp by adding *--icmp-addr* or *--icmp-ts* to hping's arguments. We'll leave that as an exercise to the reader!

Now on to the fun stuff, using hping to create custom TCP packets. Let's start off by sending SYN packets (first part of the TCP handshake) to port 80 on www.2600.com, since we already know port 80 is open:

```
[root@clotch root]# hping2 -S -p 80 -c 3 www.2600.com
HPING www.2600.com (eth0 207.99.30.226): S set, 40 headers + 0 data bytes
len=46 ip=207.99.30.226 ttl=49 id=65000 sport=80 flags=SA seq=0 win=65535 rtt=565.0 ms
len=46 ip=207.99.30.226 ttl=49 id=63206 sport=80 flags=SA seq=1 win=65535 rtt=530.6 ms
len=46 ip=207.99.30.226 ttl=49 id=26539 sport=80 flags=SA seq=2 win=65535 rtt=490.5 ms

--- www.2600.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss round-trip min/avg/max =
    490.5/528.7/565.0 ms
```

OK, so we see the IP ID's are random, which we already found out earlier. We know we're getting somewhere because the flags we received were SA (a SYN|ACK), which is the second step to a TCP handshake. The SYN|ACK stands for "I acknowledge your request, proceed." We can glean more information now that we have a responding port. Let's see if we can get the uptime for www.2600.com by adding *--tcp-timestamp* to hping's argument list:

```
[root@clotch root]# hping2 -S -p 80 -c 3 --tcp-timestamp www.2600.com
HPING www.2600.com (eth0 207.99.30.226): S set, 40 headers + 0 data bytes
len=56 ip=207.99.30.226 ttl=49 id=41548 sport=80 flags=SA seq=0 win=65535 rtt=358.1 ms
TCP timestamp: tcpts=979995024

len=56 ip=207.99.30.226 ttl=49 id=24700 sport=80 flags=SA seq=1 win=65535 rtt=398.9 ms
TCP timestamp: tcpts=979995125
HZ seems hz=100
System uptime seems: 113 days, 10 hours, 12 minutes, 31 seconds
```

Not bad. Let's go a step further and see if www.2600.com's TCP sequencing is predictable or not by using the -Q flag:

```
[root@clotch root]# hping2 -S -p 80 -c 3 -Q www.2600.com
HPING www.2600.com (eth0 207.99.30.226): S set, 40 headers + 0 data bytes
1347913158 +1347913158
3604885414 +2256972256
1768794044 +2458875925

--- www.2600.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 575.8/609.4/639.0 ms
```

By the looks of it, they aren't predictable. You can tell because the first column is the sequence number itself and the second is the difference between the current and last sequence number. Just for argument's sake, I'll run the same command on a remote Windows box:

```
[root@clotch root]# hping2 -S -p 80 -c 5 -Q xxx.xxxxxx.xxx
HPING xxx.xxxxxx.xxx (eth0 xxx.xxx.xxx.xxx): S set, 40 headers + 0 data bytes
 35128670 +35128670
 35128672 +2
 35128684 +12
 35128703 +19
 35128719 +16

--- xxx.xxxxxx.xxx hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 54.6/74.6/148.4 ms
```

As you can see that host has *very* predictable sequence numbers, making them a lot more vulnerable to source-IP based trust relationships.

We can also port scan using hping! It's relatively easy. The only thing you need to do is put a plus sign before the destination port and hping will increment the destination port every time it sends out a packet. Since we now know that SYN|ACK (flags=SA) means an open port, we can tell which ones are available. Example: *hping2 -S -p +21 www.2600.com* will start sending SYN packets starting at port 21 all the way up until you kill hping. This should sound very familiar to some people. It's the same exact thing nmap does when it runs a Stealth scan. The nice thing hping has over nmap is finer destination port control. If you want to increase the destination port each time a reply is received, you just have to precede the destination port with a "+". If you want to increase the destination port for each packet sent, precede the destination port with a "++" (examples: +80, ++1). The destination port can also be modified interactively by using Ctrl+Z. You can also specify the source port with the -s flag. By default, hping uses a random source port, and increments it by one with each packet sent, but you can stop the increments with the -k flag, which means your source port will never change. You can essentially iterate through every source port and destination port available. These functions are very useful when you're mapping out a remote firewall's rules. Here's a tip to get you started: a lot of filtering devices allow any TCP traffic with the source port of 20 to come through (which is used for active FTP transfers), and any UDP traffic with the source port of 53 to come through (used for DNS traffic). Also, some old firewalls let traffic pass when the packets are too fragmented (which you can do with the -f and -x flags).

One last example that is a fun one to pull on your extra-paranoid friend (we all know that person

And H2K came to be. The Millennium was ending. And there was Jello for all.

that's filtering and logging *everything*). Run this hping command against their firewall: *hping2 -1 -a www.fbi.gov HOST* (Replace HOST with your friend's IP.) Leave that running for a few minutes, and wait by your phone. *(*RING RING* "Hello?" "Dude, I swear the FBI is pinging my webserver!")* The -a flag allows you to spoof an address/hostname. Obviously you won't be getting any traffic back, but since ICMP is a connection-less protocol (UDP as well), you are able to pull this sort of trick off.

As you can see, hping is a very powerful tool. I barely scratched the surface with this article. With hping you can do everything from testing net performance to transferring files to using hping as a backdoor! You have almost total control of hping's outgoing packets. The possibilities are virtually limitless. The best thing you can do is download hping, read the manpage, and start playing around with it. If there's enough demand, I'll write a follow-up article on using hping as a real-world application.

Links

hping - http://www.hping.org
icmp types/codes - http://dark-intentions.net/files/icmp.txt
Shouts: victim1 for the kcmo h00kup, vegac for always being leet. Thanks guys. Much love to mom dukes.

Remote Computing Secured

by Xphile

Remote Control Applications are the greatest things since sliced bread but without proper security they can quickly turn into your worst nightmare. In issue 22:2, Screamer mentions in his article "Optimum Online and You" that he merely installed VNC on his local machine and allowed users to connect as if they were on his LAN. This might seem fine to most people but for the readers of *2600* I feel that it's not, hence the reason I am writing this article.

This article will focus mainly on some of the methods to successfully secure VNC using SSH1, SSH2, and SSL while also covering correct application configurations.

VNC (Virtual Network Computing)

VNC in my opinion is one of the best remote control applications available today mainly because it's open source and it's *free*, hence it's portable and it doesn't hog system resources like PcAnywhere or M$'s proprietary software. With that said....

Laying the Foundation

The default installation of VNC leaves quite a bit to be desired securitywise but where there's a will there's a way. One of the most important things to do is gather all of the latest patches for the flavor that you have. You wouldn't want any "skript kiddies" taking advantage of the flawed authentication methods, would you? On most versions of VNC (TightVNC 1.2.9, current version as of 8/28/2003), the default settings do not limit the amount of connections coming in a set amount of time, therefore allowing any genius to run a dictionary attack on your server and in time compromise the machine.

This brings me to my next topic, the RFB (Remote Frame Buffer) which is the protocol used in the communication between the server and the client. The RFB protocol has no type of security implementation. Therefore all traffic is in a compressed but unencrypted form that can be read with a packet sniffing tool. Unfortunately there is no fix for the RFB protocol, but that will be taken care of with tunneling. Password policy is also very weak with the default installation. Hashes are stored locally on the server and encrypted using the DES encryption method, yet they use a fixed key allowing any user the availability to run a cracking tool such as VNCcrack.

Getting Stronger, But Not Good Enough

Now that we have covered just *some* of the problems with the default install of VNC, let's fix them. In regards to the multiple connections and brute force cracking, go into the advanced section of the VNC server options. There you will find under "connection priority" a setting called "refuse concurrent connections." You will want that enabled. I would also enable query console for incoming connections and the log. Since the VNC server is a well known port (5900), you might want to change that along with the HTTP daemon. The last order of business would be password policy. Since VNC doesn't require a minimum length for passwords, it is up to the administrator of the server to properly enforce a password policy that won't be easily cracked remotely or by a local user (i.e., six characters and numbers minimum).

VNC All Wrapped Up

You now have a secure VNC server running and it's completely safe, right? Not exactly, but you're almost there. Since we now have a pretty strong install of the VNC server configured, it's time to take care of the RFP protocol problem. To do this we will use virtual tunneling using SSH or SSL.

SSH and SSH2

Before we start I must stress that you get the latest version of the SSH server of your choice and that you apply all patches. That being said let's get into the specifics. For my example I will be using OpenSSH 3.6.1., which contains both SSH1 and SSH2 suites. Once OpenSSH is installed you must configure the server to "wrap" all instances of the VNC server so that all information that is passed through to the VNC server goes through the SSH server first. The first step in the process is to reboot after installation so that the service (SSH or SSH2) will start. Next you must manually tunnel all connections using the CL. Load up CMD.EXE and insert the following command:

ssh -L 5900:localhost:5901 localhost

-L initializes local port forwarding so the servers can communicate. 5900 is the default VNC port. localhost is the machine running the server.

This will create the virtual tunnel. The next thing that you will want to do is get yourself a good SSH/telnet client so you can start the SSH session. After you have logged into the SSH server, load up VNC viewer and connect to localhost::5901.

SSL

If you do not wish to use SSH or SSH2 to tunnel your VNC connection, there is always the option to use SSL for the tunneling, but it's a bit more complicated. Stunnel and OpenSSL will be used in the following examples. The first step would be to install OpenSSL and all packages and updates and then on top of that install stunnel (for stunnel to work properly it must have some sort of SSL library, in this case OpenSSL). This is where the tricky part comes in. You will have to find the file "stunnel.pem." It's located in the \system32 folder. The next part was taken directly from stunnel.org and I give full credit to the author of the configuration file as follows.

```
PORT]
 client = no
 cert = stunnel.pem

 [vnc]
 accept = 7777
 connect = 5900


VNC servers]

 client = yes
 cert = stunnel.pem

 [vnc]
 accept = 5900
 connect = xxx.xxx.xxx.xxx:7777
 [vnc2]
 accept = 5901
 connect = 192.168.0.8:7777
```

```
LIBEAY32 DLL  1,379,459 12-31-02  11:54a libeay32.dll
LIBSSL32 DLL    476,329 12-31-02  11:54a libssl32.dll
 OPENSSL EXE  1,089,536 12-31-02  11:54a  openssl.exe
 STUNNEL EXE     59,904 01-12-03   4:54p  stunnel.exe
 STUNNEL PEM      1,690 02-28-03  12:24a  stunnel.pem
```

Once you have this in the configuration file you now must start the service. The final step in this process is to load up VNCviewer and put in the IP address of the machine you are trying to connect to. You are now finished and fully encrypted.

Conclusion

Security should be a concern for everyone, not just the computer savvy network administrator for some Fortune 500 corporation. I hope this article has given you the tools and foresight to secure your remote connection.

All software was used under Windows but there are of course UNIX/Linux versions.

Shouts and Thanks: DigitalX, Somefun, JimmyBones, Decoy_0ct, Poundofflour, and most of all eagelspeedwell for guidance.

Speech

Getting Around the System

Dear *2600*:

My parents would not allow me to sign up for a broadband connection. Dial-up, they said, was good enough. Well, what self-respecting *2600* reader would be satisfied with that? No way.

My local Best Buy had a great sale on wireless routers. For less than a good deal price on an ordinary cable router I got a combination wireless/cable router.

I sold the router to a neighbor (who has a broadband cable Internet connection). He couldn't wait to take it off my hands for what I paid for it - what a deal. I even gave him the bill and rebate slip.

The minute he hooked it up I was online at high speed with a wireless card. Sure beats ordinary dial-up. Ha ha ha.

Evil Alex

Wireless connectivity has liberated many from various forms of wired tyranny.

Dear *2600*:

I am so happy I started to subscribe last year. Thanks for such a great wealth of information.

I'll be submitting some info on poorly kept phone lines at campgrounds as soon as I make a protected cable that isolates my data port from phone lines that could have high voltage from the poorly kept electrical lines.

In the meantime I find myself in Times Square at a rather nice hotel. In the room is a primitive "computerized" mini bar full of wonderful things! I believe it's a standard fridge with a little customization from Room Systems Inc. of St. George, Utah.

Every time I open the door, it beeps at me. When you take an item, it registers and adds to your room charge. The only way it knows if you remove an item is that it trips a switch that must be depressed in order to remove any of the items.

The switches are so primitive that I can see they are N/O. Removing the wire to the switch would be too easy thereby leaving it still N/O. I could cut one of the wires, but that's destructive. We do not destroy.

Remember the beep each time the door is opened? There is no lever switch such as would turn a light on and off. But wait, what's that? Two objects that align when the door is closed. You don't suppose one is a poorly hidden magnet and the other a poorly hidden magnetic reed switch do ya?

Here's that hack. Pry out the magnet with the cork screw provided in the mini bar, hold it next to the reed switch, and none of the beverage switches care if they are depressed.

I know I'm no longer depressed.

Rifkey

It may work to defeat the automated system but nobody has yet found a way to defeat the person who comes around every day to restock the thing.

Dear *2600*:

A quick story that ties in both your 20:3 editorial and scissorjammer's letter (page 50) on the classic pull-the-battery-to-reset-the-BIOS-password trick.

Playing in the garage with high voltage one day (a PC power supply and an automotive ignition coil) I found that our GE electronic-control built-in oven was now giving an error code and beeping. Unstoppably. Annoyingly. I had probably coupled the HV into the same circuit as the oven. I figured I had toasted something. The house circuit breaker stopped the beeping (good) as well, of course, as the oven (bad).

I called a repairman and found that the cost would be $400 to repair but he didn't have the part. Being "between jobs" I decided to simply disable the electronic oven and continue using the (undamaged, simpler) two-mechanical-knob built-in oven below it. A reliable analog backup.

Making sure the circuit breaker was still off (three phase AC can really ruin your day), I got behind the touchpad by removing a few screws. Inside was the (real) manual for technicians, which was an interesting read. There are special keypresses to enter modes that let you change to 24 hour time, centigrade, etc. Also a few diagnostic procedures, the resistances of various heating elements, etc. Nothing immediately useful though.

Before trying to find and unplug a connector to the beeper, I did a standard debug procedure - reseat the connectors, of which there were many. Well, when I unplugged and replugged a ribbon cable and powered up the oven, it worked! Somewhere in there was a battery supplying power to the confused electronics, maintaining their confusion.

Clearly GE decided that it's better to retain the time of day through a power outage than to truly reset the system from a soft error when it power cycles!

One more comment on the Northeast blackouts and hackers. During one of the last worm storms, a power plant did get knocked out. Yes, they had firewalls. But a consultant's machine had a connection and the consultant got the worm.

Important systems should be secure, and this means an air gap. (Reportedly the NSA uses faxes, not e-mail for public correspondence because faxes don't leak accidentally and don't carry malware.) Possibly also analog backup control or safety systems. As you editorialize, there should always be true redundancy for important things. (Robust server farms have connections to different backbones that come in via different parts of the building to avoid the killer backhoe single-point-of-failure.)

Khoder bin Hakkin

Miscellaneous Fact

Dear *2600*:

Now you can see what time it is in the *2600* timezone: http://time.gov/timezone.cgi?2600/d/2600. Interesting....

SFG

New Ideas

Dear *2600*:

I have been an avid reader for longer than I remember and I love your magazine. I really think that I can contribute somewhat to the magazine. I am a really big perl programmer and a long time OpenBSD user and administrator. Also, my girlfriend is the editor of a local paper so I can have her help me write. If you think that I can contribute please feel free to e-mail me. I will be happy to do anything to get a small article in one of the issues.

Erik

It's important that you have an idea that you're willing to pursue and turn into an interesting article. We can't assign this to you as it has to come from your experience. We can give you advice and tell you that it should be about something you're familiar with that would be interesting to others who have some knowledge of this field. And most importantly, it should have a hacker theme that encompasses the quest for knowledge, the desire for experimentation, and the bypassing of artificial and ill-founded constrictions.

Dear *2600*:

I was just curious whether you had heard anything about the start of a campaign to unify the hacker community with one logo? I would be interested in writing an article about this (and also know there are t-shirts already available with the proposed logo at www.shirtsbymail.com). I am not an excellent writer but am just proposing the idea and wondering if you had heard.

Chris

If hackers were all part of a major corporation it would make sense to have this sort of standardization. But fortunately they aren't. They're a very diverse group of individuals who share some common values but have many different perspectives and ways of doing things. This means many logos and other forms of art to express who we are.

The State of Education

Dear *2600*:

In 20:2 four middle school girls wrote *2600* about the "dangers of chat rooms" and how "it is strange that there are still organizations that promote the use of chat rooms" due to their evil nature. I have never heard of such brainwashing taking place within our schools. According to these children's instructor(s), bad things happen in chat rooms to unsuspecting children, therefore chat rooms are evil. If our schools are going to apply that logic, it should be applied to other technologies as well, like television and computers. Every day almost every person in America, and all over the world for that matter, can turn on their televisions or logon to the Internet and "see" things that could be considered "harmful" to them. It amazes me that these instructors fail to point this out to their students and state that these methods of communication are bad. Consider the example of privacy. Their logic could also say "people who do illegal or unethical things often do them in private. Therefore everything that is done in private is bad or wrong."

If they can brainwash our children into believing that chat rooms are bad they can brainwash them into believing that many of our "inalienable rights" are wrong and should be willingly given up for the sake of safety. The potential is frightening.

richard

Dear *2600*:

In the last issue of *2600* you printed a letter from some girls doing a report on *2600* or something along those lines (can't exactly remember). When I read it I wanted to cry. There is something seriously wrong with the American education system if they were serious.

Muttski

Dear *2600*:

Because of all the letters on the subject that I have read in recent issues of *2600*, I would like to comment on the issue of school districts and their policies on web filtering.

I am a network administrator for a school district in South Carolina. Our Internet circuits and WAN circuits are funded by the state. If we do not provide some sort of filter to prevent students from accessing pornographic and hate material, the state will pull our funding for Internet access and the students will have *no* access. We do, however, have some say at the district level over what other types of content get filtered. I have specifically added 2600.com and other sites like it to the "approved" list in our filter.

When teachers or students notice that a site they need to access is being blocked, I check it out and allow access. I encourage students in our high school computer and network technology class to learn more about and participate in the type of "hacking culture" that your publication supports. I know this letter isn't very informative. I guess I just wanted to let you guys (and your readers) know that not everyone that works in "the system" is a bad guy. Some of us simply have to walk the thin line of protecting our kids while still letting them experience the world of information that the Internet and sites like 2600.com provide.

lord_stinkington

Dear *2600*:

I need help. I stay at a college dorm at a small private university in south Florida and they regulate the network like nazis. Today they blocked all ports and servers for IRC. Last year they blocked kazaa, tesla, winmx, etc., etc. I am not a computer guru when it comes to such technical aspects as networks and

And H2K2 was bigger than all the rest. And it was good.

servers, but I do know more than the average PC user. Please give me some advice or link me to a tutorial where I can configure a backdoor so I can chat on IRC or download music. I understand that universities don't want students sharing files, but to tell us what and where we can download or chat seems unethical. Today I made an appointment with the director of my dorm. Earlier I tried getting appointments with the dean but I was redirected further and further down the ladder of authority.

alex aka Suge

A number of people will tell you that it's the university's network and they can do as they please. But this is only partly true. You are, after all, an important part of the university and your money helps to make this network possible. So your input should not be ignored. The fact that so many people accept this is why it seems to be the norm today. Before you resort to back doors, do everything you can to expose the ignorance of your school's policy. It might open some eyes and make a difference.

Dear *2600:*

I attend a college of about 2900 people. When I first got to school I was looking forward to a fast network that I could use to learn efficiently. Instead the network is slower than an ISDN line. Not only is it slow but they also require you to register your computer on the network in such a way that they have the ability to track everything that you do on the web or on your computer. I feel that this is wrong but I would like to have your input on the subject and what I might be able to do about it. Thank you for your time.

Sheff-Boy-RD

If you feel that it's wrong you have every right to make an issue of it. As mentioned above, you're paying for this network and you have the right to expect a certain standard of service as well as protection of your privacy. You don't have carte blanche to violate their policies but you can make sure that everyone knows why you believe they need to make some changes. And in many cases, people won't even be aware of these issues until someone brings them up.

Military Readers

Dear *2600:*

"Is it forbidden or risky to receive our magazine while in the military?" I have a friend in the Indiana National Guard. I asked him about it. Yes, the magazine would be confiscated, and second, they would put him/her in confinement to clear their head for a few days. No court martial of course, unless it was a repeating incident.

Neo

We can only hope you're kidding.

Dear *2600:*

My husband reads *2600* in Iraq. Please don't print my name.

Noname

Dear *2600:*

I'm just reading the letters in 20:3. You ask if it's forbidden or risky to receive your magazine while in the military. I'm a tech in the Canadian Armed Forces, and every time there is a new issue of *2600*, it's very quickly passed around the shop.

PhatMan

Dear *2600:*

In issue 20:3 you responded to c0l0r3dfr34k asking if it is forbidden or risky to receive *2600* in the military. I can only talk about my experience but, so far, possessing the magazine has been no problem. I have a lifetime subscription which is sent to my home and I then have it shipped here. Of course, Websense blocks 2600.com as "hacking" and they do frown upon any creative ways of maneuvering around Websense. I'm currently deployed in Kosovo and I got away with using https://nav.ebutechnologies.com for about four months before G-6 (the Army's communications department) caught on. My primary use for Ebu was getting my weekly fix of *Off The Hook.* I guess I won't get to hear OTH again until I get out of here in March. Whether or not anyone on base knows anything about *2600* or not is anyone's guess, but I wear my Blue Box t-shirt with pride whenever we get to wear civilian clothes. My experience is my own though, and anyone with an asshole for a boss may very well get in trouble for possessing this "contraband." I'd like to hear other stories about this issue.

On a related side note, it is interesting to point out that the Constitution that we are sworn to protect doesn't apply to us when on active duty. We are under the Uniform Code of Military Justice. Things work a little bit differently under the UCMJ, usually to our disadvantage. Thanks for the great mag, *2600.* Keep up the excellent work.

karniv0re

Dear *2600:*

In response to a letter in 20:3 where you wondered if the military can get *2600* mailed to them, the answer is yes. *2600* is mailed in discreet brown paper coverings, like any self-respecting hate or porno mag, so no one is the wiser. Also, depending on the proxy server at your work section, you might even be able to surf on over to the 2600.com website.

Cpl Grimes
USMC / 2171

Miscommunication

Hi,

You have contacted the RunCoach Mailing List. You request has been passed to a human for interpretation. A response should not take too long.

Regards
List Robot

We've done no such thing. How dare you accuse us of contacting you. If you weren't merely a robotic script, we might entertain the notion of exacting some sort of revenge upon your ass. Fortunately a human will interpret this "request" and see it for the charade it is.

Further Info

Dear *2600:*

This letter is in response to Matt's letter in 20:2. He asked about just breaking CDs into little pieces to keep others from retrieving their data. In most cases this would seem the easiest and most logical thing to do, although not the most efficient. Anyone who can afford them (governments) can use magnetic sensors and electron microscopes to grab any information off any disk. The individual(s) looking to grab data off of your smashed to pieces CD can piece the CD back together to the best of their ability, then use one of the aforementioned devices to pull the data from the CD. Electron microscopes can even be used to view files that have been deleted *and* overwritten on your hard disk. If you are looking to hide information that was on a CD from your friends or family, go ahead and mash it to your heart's content. If you are looking to hide from the big guys with the cash, I'd recommend a nice bucket of acid.

DeadPainter

Dear *2600:*

Your magazine recently featured an article on microwaving a CD to destroy it. There is an easier method. Get a piece of sandpaper and sand off the top surface (the side you write on). The reflective layer comes right off and you're left with a clear, hence unreadable, plastic disc.

Anonymouse

Dear *2600:*

In 20:2, Jason Argonaut presented a technique for recovering the Administrator password on a Windows XP system. That approach certainly works, but a much faster way is to simply use chntpw. chntpw is a Linux utility that is designed to reset the password for any account on a Windows system. You do not need to know the old password in order to set a new one. You simply boot the target system with the provided Linux boot floppy and follow the on-screen instructions. In less than 30 seconds, you can reset the password for any account that you want. chntpw is available here at http://home.eunet.no/~pnordahl/ntpasswd/.

miniz003

Dear *2600:*

In 20:2, Jason Argonaut outlined a way to gain access to your Windows XP system should you forget your administrative password. This works, but it's a tad lengthy, and unnecessarily so at that.

The way Microsoft recommends (yes, Microsoft tells you to do this) is to boot off a floppy and use the dos mount program of your choice to mount the hard disk and then delete the local security hive, which will remove all user accounts from the system, and when XP (or pretty much any other version of NT 5, which include Windows XP Home and Professional as well as Windows 2000 Professional and the three varieties of Win2000 Server) restarts, it will notice the hive is gone and replace it with the default, which is (drum roll)... an account named "administrator" with a blank password. I *believe* - and don't hold me to this - that this will remove only the system accounts, so your Active Directory in the case of a server *should* be fine, and if you're on your personal PC, the only account you probably use is your admin. But please for the sake of god back up your stuff. With AD this of course means replication.

If for some reason you've set up some really elaborate permissions profile for each user you set up on your personal computer for god-knows-what-reason, Jason Argonaut's methods would probably be just as or less stressful than recreating your permissions again, but I assume you just want to get back to playing Half Life or something....

It is really incredible how much Microsoft will give away about its security misfeatures, by the way. If you forgot a local administrator password on an NT 4.0 client for example, there was a method in which you knowingly typed a nonexistent domain name in the domain field and clicked connect, then clicked one of the corners of the "domain not existent" message box five times or something like that, and it would log you in as the computer admin. I don't remember it verbatim, but the interesting thing is not the exploit itself but where it can be found alongside the aforementioned XP one (if it's still there): on Microsoft's own searchable tech help site, TechNet (www.technet.com).

Looks like that MCSE training course *was* good for something.

Slacksoft

Dear *2600:*

After reading "Fun with the Nokia 3360/3361" from 20:2 I coincidentally went to my local Cingular Wireless store to change my contract (and phone). After getting the contract I wanted, I told the man that I did not want to program my phone just yet since a relative is using it at the moment elsewhere. The man agreed and showed me how to program the phone. The steps were: 1. Dial *#639#, 2. Enter the 10 digit cell number, 3. Enter 00024 (doing some research I found out this was the System ID from the service provider), 4. Restart the phone. That is it. This code was for the Nokia 3590 but it seems to work with most, if not all, Nokia cell phones (the access code, not the programming itself). Same goes for *3001#12345#. I did not want to attempt to program another cell phone with the fear that it could become a homing beacon.

And on another note, no more howtos on web servers from cable/DSL! You printed three of them in the last year!

hbob

Dear *2600:*

I would like to thank XlogicX for the intro article "Hardware Key Logging" in 20:2. He provides pros and cons, an intro to a commercial key logger, and some theory for building one. XlogicX explains that hardware keyloggers will record all keystrokes until it sees a password typed out, then the logger will repeat all of the keys it saw. I would like to offer an idea to those who are capable of constructing a full-fledged logger. Not only could a logger receive information from a keyboard, but it could also receive information from the computer. Since the computer can control the keyboard's LED lights, the logger could monitor these actions and react on them also. The LEDs could be flashed and toggled in a certain order to instruct the logger to start recording keystrokes, to stop recording, to replay keystrokes, etc. The one downside to this is that there would have to be an extra program, executable, script, whathaveyou on the computer to not only control the LEDs, but to create the certain flashing sequences you need. But as an added bonus, because the logger can be controlled by the computer, and because computers can be controlled remotely, your logger could be controlled remotely also. Hope this helps.

mrbrown8

Dear *2600:*

I just wanted to add some info related to Bill Melater's article "Xploiting XP" in issue 20:2. Near the end of the article it is stated that if you change out more than three pieces of hardware, XP Pro will ask you to reactivate. This is maybe true but is definitely in no way a problem. I have a legit copy of Windows XP Pro Corp. that I got from my university prior to sp1 (sp1 is different as we just negotiated a new agreement with M$). I have applied the service pack and have had no problems nor do I foresee any if I were to replace hardware. My reasoning is due to the fact that I have had this same copy of XP Pro installed on a completely different machine. So you may have to reactivate but that would in no way cause a problem. You could just reactivate using your same activation code. Since all of my university's CDs prior to sp1 had the exact same activation code, there would be no way to for M$ to tell what was going on, let alone engineer a way to render my legit code nonfunctional. If you have a volume license key then as far as I can tell you should be good to go until Longhorn.

Sparklx

Dear *2600:*

As a little follow-up to Lucky225's excellent article on social engineering to gather information, a nice trick if you have a cell phone number would of course be to apply the same tricks to the cell phone provider. But the big question is, who is the provider? A great way to find out is to visit the major carriers' web sites (Verizon Wireless, Nextel, Cingular, AT&T Wireless, whatever other ones you can think of) and try to send a text message via the web (you would, of course, want to do this from an anonymous web sort of site if you would rather this not be traced). You will receive an error message indicating that the phone service is not with a particular provider if they are with one of the others. Through process of elimination, you can eventually find out who they are with, then contact that company to get the information you need.

Somar

It's also getting harder to differentiate cell phone numbers from regular land lines as portability now allows the latter to become the former.

Dear *2600:*

About semicerebral's ordeal with his Sony MiniDisk... although I am not familiar with his particular model, all of my MiniDisk equipment, portable and AC powered, includes a TOSLINK port (optical SPDIFF). Using the proper cable (right - available from Sony of course), you have digital output to whatever device you wish to use. It seems nearly all of the new "hyper threading" motherboards offer optical SPDIFF on their soundcards and that could save you a chunk of change as I bought into MiniDisk when it first appeared and I have purchased at least two expensive PCMCIA cards to allow optical transfers from my portable MiniDisks. I too am a musician, play in a band, and have achieved some truly great results using MiniDisks as recording media. Massage the results with a little Sound Forge (oh no - Sony just bought Sonic Foundry too!) and you will be amazed. Tip: I got two tiny special "binaural" microphones and hot-glued and siliconed them to a pair of fake glasses (the lenses are plain glass) and, unless you study them, you cannot tell the mics are there. Wired to my trusty MD in pocket, I have found that the resulting recordings sound as close to what I remember they did as I can imagine. Your struggle with the free software that came with your unit comes as little surprise. You get what you pay for - it's free. Get a real program like Forge if you want to extract the best from your unit. It'll transfer analog (as you're doing now) or digitally via TOSLINK and you can edit, add effects, normalize, etc. and save these efforts as .wav files, ready to burn to CD. Now circumventing ATRACK (Sony's nasty copy protection scheme) is another story. Cruise Google. I hacked ATRACK years ago as it was a massive butt pain from the start. One other suggestion: purchase a "home" MD unit to extract your music from MD via TOSLINK and don't worry about the portable unit!

Taurus Bulba

Dear *2600:*

In response to PhrenicGermal's letter about OS 10.2. Holding down the "command s" key combination on boot will drop you into single user mode. Single user mode is a special mode available on most *nix systems in case of horrendous massive failure during normal operation. The idea being that if some crazy fdisk command you do breaks your password file or some other such nastiness, you can recover. The reason you couldn't change any files is because darwin mounts the root filesystem in read-only mode during single user mode by default. This isn't much of a problem because you can use the mount utility to remount the root partition in read-write mode. Some other interesting facts: This works on 10.3 as well (I checked it as I was reading the last issue), and you can spot the original copyright notice from Berkeley after the initial boot sequence. This isn't really a security flaw for most OS's as arguments passed to the boot loader are what trigger single user mode. For most people with multiple users with physical access to the hardware, locking the bios and the boot loader will keep them from easily rooting your box. For OSX, you'd have to fuddle with the BootX boot loader to keep them from dropping you into single user mode, which I wouldn't know how to do if it can be done. It might even be a firmware issue depending on what kind of system you have. Good luck to all you OSX hackers out there!

Hroly

Dear *2600:*

I just read PhrenicGermal's letter in 20:3 about getting single-user mode on Mac OS X. It's true, it's root, it's easy; a great many unix flavors have similar "features." It's a handy feature for emergency administration work when you're really fsck'd. It's easy enough to defend against if you're concerned. Just go to http://www.apple.com and search for "open firmware password". It's a utility which will block single-user mode, and cd-rom boot, and netboot, and target disk mode, and verbose mode, and... you get the idea.

Scott

Misdeed

Hi,

You have been subscribed to the RunCoach Mailing list. This is a very quiet list. The next announcement should be in a few weeks regarding the next beta release.

Regards
Paul

Now you've done it, Paul. You share the same DNA as the humans on our staff yet you act as if you were an automated process working as an agent of the robotic script. This to us is nothing short of treason. Had you read our automated response you would have seen no indication of any interest in your lame-ass mailing list. Yet you betrayed your humanity and signed us up anyway. We cannot forgive this. Our readers cannot forgive this. What's more, the human race will never forgive this. Prepare for what lies ahead.

Pointed Questions

Dear *2600:*

I was just about to buy a *2600* hoodie and *Freedom Downtime* but then I saw it is only on VHS. I do not have VHS anymore. Do you have any idea when it is going to be released on DVD? Or if not on DVD do you think you could encode it to Divx or mpeg and put it on a CD? Is the reason that you might not want to release it on mpeg or DVD because it will end up on P2P networks? I think we should be able to choose the format that we view our media in. Is that not the reason you were fighting for DecSS?

TrIpAnDaNce

Just calm down. We're not trying to keep anything out of your hands. We're busy working on the DVD and it will be out soon. If you don't want to pay for it, the film is on the net in all sorts of formats. We've already said we don't mind. If you can't track it down, that's not our problem. We're obligated to the people who purchase the film from us and help make such projects possible in the first place.

Dear *2600:*

What's with the bottom of page 33 in all the issues? It's always different from the rest of the pages. I've looked back through several issues and can find nothing between them that establishes a pattern. Just curious.

magnum0711

We believe our readers hold the record for noticing things like page numbers. In fact, the page numbers are sometimes more popular than the articles.

Dear *2600:*

I am asking for your permission to translate some articles from *2600* to publish in our magazine called *Hacker* in Brazil. Is it possible?

Marcelo Barb

Absolutely. Just be sure to give credit to the author and to 2600. Also, please send us a copy for our library. Above all, create as much of your own content as possible so that your magazine will be unique.

Dear *2600:*

Why do hackers refer to a hacker that is not causing a problem with the system he or she is observing a "white hat" and the one who is committing a crime a "black hat?" You would think a group of ultra-liberal free spiriters would be less driven by color. Don't say it doesn't matter what color is chosen for the term because if it doesn't matter then reverse the terminology. I'm personally getting tired of white people associating crime, evil, and bad things with my heritage... especially when the white people in our society are committing most of the crimes.

Ken

To begin with, hackers are not the people coining the "black hat/white hat" phrases and using them. Rather, they are used by the people who have money to make by creating an atmosphere of fear mongering so that people buy their products or attend their expensive conferences. As to the problems you have with the actual colors that are being used, that's a language issue that goes far beyond anything we can address here. But you certainly don't help matters by continuing to label races albeit in a different direction. And finally, please don't label hackers as being allied with any one particular political view. We certainly have our opinions here but they are just that - our opinions. They may or may not reflect what most other hackers agree with. Individuals are free to make up their own minds.

Call For Help

Dear *2600:*

I am calling out to the other esteemed readers of this fine publication for some assistance. On the Nortel Networks PBX systems (Option 11C, Option 61C, Option 81C) there is a dongle and daughterboard that essentially make up the "software" portion of the switch. This is how the software release itself is upgraded by Nortel Networks, as well as adding mailboxes to the voicemail portion, etc. It is done based on

And we said, Let us go forward once more.

the serial number that is engraved in the small dongle which is about the size of a battery for an electronics device that fits on the CPU card. The serial number on the dongle is what will also come up if Nortel (or an authorized dealer with access to that portion of the Nortel website) brings up that switch serial number. *However,* I have come across a few switches where the dongle has a serial number on it, but when I pull it up on the system it's an entirely different internal serial number, typically with a higher release software level and more voicemail storage. I am calling out to any fellow technicians who may have more information on this. I know you're out there because I've come across your work. I have a few "tricks" myself that I would be willing to offer up in return should anyone be interested.

Professor_Ling

The Issue of Piracy

Dear *2600:*

After reading tack's letter in 20:2, I got to thinking. I am an avid software pirate and am always downloading some sort of pirated program, movie, music, and whatever I need/want. Some people believe in pirating software, using it in a "trial" period, and buying it if they like it. I would have no problem with this if I actually had the money to pay for software. But most places don't hire until you are 18, which leaves me without a job and ultimately no money. So I started thinking about what I would do if the MPAA came to my door. What kind of legal defense would I have on my side? Probably none. But after reading tack's letter, it seems that the guys with the MPAA aren't very accurate with their tracing. So if someone like me actually got caught, what kind of chances would they have?

fH

If you need to rely on someone else's incompetence to get away with something, you probably won't be getting away with it for very long. You also should examine your motivations. If you truly want to plead poverty, then the "always downloading" all kinds of things scenario won't wash. That scenario is more suited for someone who believes that software in general is too expensive and is downloading everything in sight as a protest. If you want someone to believe that you're just a poor student who can't afford the software he needs to learn, having downloads going 24/7 and a huge library of programs, music, and movies will really build the case against you. Not that you could get away with anything if they even find one pirated program in your possession. It's all selective enforcement spiked with greed, fear, and revenge. In other words, it's not a pretty place to be. But the outcome of this battle is going to be significant.

Dear *2600:*

A big issue regarding music is file sharing with programs such as kazaa. It seems that if organizations like the RIAA want to sue copyright violators, then people should stop using kazaa. There are several other ways of obtaining music that have not been cracked down upon yet. One method of obtaining music is to record it from the radio. This method is not the easiest thing to do and it does not provide very high quality music. Although if you are allowed to record music from the radio, then certainly you should be allowed to record music from online streaming radio stations.

martianpenguin

Most of these online radio stations have pretty crappy quality so the special restrictions aimed at them really don't make much sense. It's just the industry's fear of the word "digital" which instantly conveys to them the image of people getting perfect copies of whatever they want and never having the need to buy anything from them again. We can only imagine how crazy they will become as digital radio starts to become the standard. On this subject, we're curious if anyone has been recording music off of the satellite "radio" services (XM and Sirius) and if the RIAA has been at all concerned about this.

Dear *2600:*

The RIAA's opinions on file sharing are so over exaggerated. Who are we feeling sorry for here? The people whining about piracy are some of the richest people in the world. I'd bet if this was some poor starving artist finding their music online, they'd probably take it as a compliment, not a threat. There is so much more than just music and movies out there on the Internet, yet all you ever hear about is the media. I think this is partially because the production companies seem to be the most threatened by all of this. If people can go straight to the artist, who's going to need a production company to take 90 percent of the profit?

What's the difference between downloading music and recording something off the radio or TV? If they're going to make file sharing illegal, they should make tape recorders, DVD/CD burners, PC sound cards, VCRs, and basically anything else with recording capabilities, illegal too. The industries seem to be more afraid of change than anything else. What they should be doing is figuring out how to use this technology for their own benefit, not trying to destroy it. Imagine what would have happened had the movie industry gotten their way and destroyed VCR technology.

It's almost as if the RIAA is begging for a rebellion. Their actions of "let's sue everyone and maybe we'll get lucky" seems to have just encouraged people's downloading because it certainly hasn't stopped it. And no matter what they do to try and stop this, the technology will eventually get cracked and people will be free to trade once again. Look what shutting down Napster did. It didn't stop anything and the file trading spread all over the Internet and nearly everything is now being shared. With most of these files being shared on peer-to-peer sites that have no central location, they're basically impossible to shut down.

The RIAA's current actions are basically a present day witch hunt. It's funny, they're always talking about these evil teenagers that have no respect for copyright and other people's work. Yet a good percentage of people sharing these files are adults. I wonder what people would think if someone's 90 year-old grandmother was busted for file trading. Because you know she's out there somewhere, waiting to get caught. Maybe we need something like that to happen, just to prove how ridiculous all of this really is.

Jeff

It's already happened to senior citizens as well as to a 12-year-old. Considering the RIAA is involved in marketing some of the biggest performers in the history of mankind, they certainly should be doing a better job marketing themselves.

Dear *2600:*

Love your magazine and will continue subscribing to it for the rest of my life.

I just wanted to comment about your response to eigenvalue's letter in regards to software piracy. I completely agree with him. As a shareware author myself I do know the problems of copyright infringement. It's not "theft" but someone has broken the terms of which I published the software.

Price, limitations, terms, etc. are up to the author. If you don't agree with them, if they are inconvenient, or if they are plain stupid, then don't buy it *and* don't use it. No one gives you the right, just because you disagree with them, to trample over their rights. If I write a computer game and charge $10 for it, I expect only you (or a very close circle of acquaintances) to use it. It does not give you the right to give it out for free to hundreds of people. Also, if you can't afford my (reasonably priced!) software or are cheap, it does not give you the right to hunt down a warezed copy. Find an alternative, write your own, or do without it. At worst, contact me and let me know. We can always work something out.

Luckily I have not been the victim of (massive) copyright infringement. I sell my software for a fair price, I provide good support, and because I'm a pragmatist, I spent quite a bit of time protecting my software from cracking (I send personalized copies to each user with their name/address).

Don't get me wrong, I also have freeware; either stuff that I designed to be free, or things that are older and not as attractive to folks nowadays. But I have to pay the rent and feed my kids, so if I ask for a fee, I'd like to be paid for my labor. I treat my customers with respect and courtesy. In return I expect the same.

If Adobe, Apple, MS, etc. aren't doing the things you want them to, don't use their stuff. Use Gimp, Paint Shop Pro, OpenOffice, or borrow a friend/library/Kinko's computer temporarily. Just because they have millions of dollars, it doesn't give you the right to infringe on their copyrights. I personally boycott a lot of companies I disagree with (for example music CDs), and my life would be a lot easier if I just went along with the herd. But at the end I (still) have a choice, even when it means I have to do without something.

By the way, your friend could have posted in a Mac newsgroup or a forum to find out if FinalCut Pro would work on his older system. What was he expecting? An honest answer from a store that wants to shift as much hardware as possible? When spending that much money one should do a little bit of research prior and not blindly trust a sales person.

Hooky1963

You raise very good points. The people who write software independently of the large software houses have a much more direct connection to the effects of piracy and we should listen to their experiences. We would be hard pressed to come up with a reason why someone shouldn't support this kind of endeavor by paying the requested price for the software. But you put forth a number of interesting phrases. You say your software is "reasonably priced." Supposing it wasn't. Would that change anything? You suggest that people contact you if they can't afford a copy so you can "work something out." It's great that you care enough to make this offer but what about those who don't provide this option? What if you didn't treat your customers "with respect and courtesy?" Would that give people the right to copy the stuff on their own terms? We think not. But we do believe it would nonetheless become prevalent and you would be a very bad businessperson if you couldn't figure out what you were doing wrong that enabled this kind of behavior to flourish.

As for the Mac question from last issue, we should all expect honesty from those we do business with. While obtaining a pirated copy of the software wasn't honest either, we're hardly surprised that someone resorted to that after being consistently treated badly by the Apple representatives. If a product is good and if people believe in it, we're convinced that they will support it as long as it isn't priced out of their range.

Some Clarification

Dear *2600:*

This is a response to Chris McKinstry's 20:1 "A Hacker Goes to Iraq" article. What the heck is he talking about? I'm in the US Army Signal Corps. We provide the backbone for communications all over Iraq. I can tell you firsthand that computers are not a foreign concept to Iraqis. Chris makes it seem like his book and description of computers are going to wow the Iraqi people. I beg to differ.

To put it in perspective, in April I was in a store in Kirkuk buying 256 MB USB flash drives for my unit. Also available in the store was every app and game written in the last five years. I'm fairly certain that all the software was illegal since for one US dollar you could have any application burned to a CD... but that's not the point.

The point is that the store existed. The point is that Iraqis use computers. The point is that Chris is no great missionary that's blessing Iraq with his computer teachings. Where there's a will, there's a way, and the Iraqi people found a way apparently long before we ever showed up.

I won't go into detail on the invalidity of his implications that we target hospitals and water plants. I will however mention that we've established uncensored Internet cafes in downtown Tikrit and in other cities. The usage is amazing. The job gets difficult when people shoot at us, but we get the job done nonetheless. Why? Try to follow me here because conspiracy theory won't explain this: the government is made up of humans too. A wild concept I'm sure. Bombs aren't the only thing the government delivers. I'm providing

And so, without fanfare, we announce

Internet whilst my comrades do their part building hospitals, training police forces, and building water treatment plants.

So, that's my non-pacifist perspective. If it's not apparent by this point, I took great offense to the article written by Chris. Iraq's on-line because we've worked very hard and removed those who impeded free information flow in the past. I'd love to hear an update from Chris so that we all know how he's doing with that book. Oh, and if you're an Iraqi who has yet to be enlightened by Chris and his copy of *Creative Computing,* you can view it on-line at: http://www.atariarchives.org/bcc1/ but you probably already knew that.

By the way, your magazine is a big hit in our unit. The cover seems to draw everyone's attention and I find even those lacking any hacker skills or deep computer interest reading it from cover to cover. Keep up the great work.

Mark A. McBride
http://www.markmcb.com/

Dear *2600:*

In 20:2, page 42, in ddShelby's article "802.11b Reception Tricks," I noticed an error: The acronym BNC, used to specify a particular style of coax antenna cable connector, is said by Mr. Shelby to represent "British Naval Connector."

Now that is not the real origin of the acronym, nor is the Royal Navy in any way responsible for the connector. European radios (British-made ones included) do not even use BNC connectors for their antenna connections. Strangely enough, ddShelby's was not even the first erroneous story I have encountered regarding the apparently cryptic designation BNC - I have also heard it said that BNC is supposed to stand for the initials of the two unnamed Motorola engineers who designed the plug.

Well, the truth of the matter is that the acronym really stands for "bayonet N-type connector," and the device, like very many other standards in the modern radio communications business, was developed by Motorola, an American concern. The appellation "bayonet" in fact refers to the action employed to fasten the connector together; a pushing-in and twisting motion, not unlike that used by a soldier killing an enemy by use of a bayonet. So the name has military origins, if not the plug! A bayonet fastener employs two tiny pins on either side of the male end which fit into two sorts of spiral-type grooves or channels in the female end which lock it into place when the connectors are pushed together and the male rotated a half turn clockwise. Bayonet-style fasteners are also used on small light bulbs, plugs, sockets, and other devices (many of which were popular on old 1950's and 1960's era electronic instrument panels) which all fit together by pushing in and twisting a half right-hand turn.

The "N" part of the acronym indicates the actual type of connection made between the conductive elements of the cable - it doesn't mean "Naval." There is an entire series of alphabetically-designated connector types, including "A-type" (also mentioned by ddShelby in his article was the SMA, or "SubMiniature A-type") and, perhaps most popular, the "F" type used in TV antenna coax, cable television, and VCR connections. In an "N" connector, there is a sleeve and cuff that fit together to connect the ground conductors.

Thus, BNC = Bayonet N-Connector, just as TNC = Threaded N-Connector, which ddShelby actually did identify correctly. I half expected him to follow through with his nomenclature and claim it meant "Taiwanese Naval Connector" or something. (Just kidding, dd, a little good-natured ribbing is indeed in order in situations like this.)

There are even just plain old "N" connectors that have no mechanical device to hold the plug and socket together, besides simple friction.

Just thought I'd clear up that little bit of info. Not to knock ddShelby, of course. In fact, I thought his article was otherwise extremely well thought out and researched, and appeared to have at its basis good, sound scientific experimentation. He went through much more trouble than I ever would have to experiment with 802.11b antennas.

By the way, if anybody would like to learn more about all kinds of radio antennas (microwave or otherwise), pick up *The Antenna Book,* published by the ARRL (American Radio Relay League). It is excellent and it contains many hundreds of antenna designs, including yagis, dipoles, log-periodics, etc. And all the mathematics necessary to calculate such things as gain, SWR, harmonics, etc., as well as to design your own specific-purpose antennas.

Hey, many of us hams are hackers, too!

Colonel Panic
a.k.a. KC9EQK
a.k.a. John

We appreciate your obvious passion on this issue. However, the author is far from the only person who attributes the BNC acronym to British Naval Connector. This is widely considered to be an accurate definition, as is Bayonet Neill Concelman. Hopefully there won't be wars fought on this subject anytime soon.

Dear *2600:*

This is regarding "Basics of Cellular Number Portability" in 20:3. C3llph's article is basically right, but he (or she?) is clearly a bit confused about number portability. The MDN (also known as MSISDN in GSM) is simply your phone number. There is very little purpose to having this in a phone, which is why most analog, TDMA, and CDMA phones don't have it. The MDN definitely is not used to "identify your phone on their [your provider's] network."

A minor error is that SOC is not "Start of Cell." It is the System Operator Code and identifies the cell provider for TDMA phones only. See www.tiaonline .org/standards/soc/soc.pdf.

The MSID is a short form for MIN (Mobile ID Number) or IMSI (International Mobile Subscription ID). IMSI is the number used by GSM providers to identify phones when placing or receiving calls. MIN is used by analog, TDMA, and CDMA or, for newer phones, IMSI can also be used. MIN has always been programmable, although in the old days it was by a chip that had to be removed from the phone.

MIN is a ten digit number that is usually the same as the MDN. Although the MDN is variable in length - sometimes you only dial seven digits of it, sometimes 11. The MIN is always ten digits, plus or minus 0. That is, the MIN is usually the same as the MDN in the US but not in other countries. It is certainly true that with number portability the MDN will stay the same, but the MIN will change to reflect the new provider, meaning that the MIN and MDN will not be the same. The website mbiadmin.com has some interesting stuff on this.

The description of routing in C3llph's article is not very accurate. Someone calling you dials the MDN. The call is sent through a long distance network and, just before it reaches your old provider a Number Portability Database is asked whether the number is ported. If it is, a Location Routing Number (LRN) is provided. This is then used for routing and the call is directed to your new provider. The call never goes through your old provider.

If you're roaming, the new provider contacts the provider at the place where you are (yes, cellular systems track phones all the time). That system provides a routing number to your new provider. The call is forwarded to that number. When the call gets to the system currently giving you service (say, in another city) the routing number is mapped to your MSID which is used to page your mobile.

Complicated, sure, and who knows what will break when you port your phone number. There might even be infinite loops where a call bounces back and forth between your old and new providers forever. But, for sure, it was complicated even before porting. It is just worse now.

D1vr0c

Dear *2600:*

In 20.3, C.B. Cates wrote a good article about ripping off Blockbuster by way of calling in a wrong-store return. Actually quite intelligent, but Blockbuster has been aware of this possibility for quite some time and they're starting to train their employees to treat every wrong-store return as if it were a fake. There's a distinct and meticulous method and systematic answer-and-response now that sounds more like exchanges between KGB diplomats half a century ago than employee interaction at a rental store. Also be aware that any employee (and certainly manager) with any sense will know the store numbers and addresses of most every store in the district. And, if not, they're all listed by the telephone in the first place. Best of luck, but know that the prospect of this working is dropping quickly, especially with the amount of shrink many stores are getting.

Poetics

We're glad they got the wake up call.

Dear *2600:*

In 20:3 "spite" writes about the Xbox and things you can do with it. What caught my eye is that right off the get go he proclaims the Xbox as "Microsoft's first console outing." This is not entirely true. Microsoft has a history of getting their hands into everything, and doing it in the fine print. In the early 1980's (1983 to be exact) ASCII worked with Microsoft to produce the MSX home computer console standard. There are a lot of speculated meanings for the acronym MSX, and even the original manufacturers that followed the MSX standard disagree upon a single variation. The acronym, however, is not important. By the time the MSX group of manufacturers was gearing up to release the second version of the firmware (MSX2), Microsoft deemed it a failure and went back to fulfilling their lifelong dream of causing the average consumer hours of frustration via wonderfully crafted blue screens. Just goes to show, a little research and you'll find that Billy was a very busy boy from the start.

phresno

Spreading Knowledge

Dear *2600:*

I am a consultant here in the Portland, OR and Vancouver, WA area. On all of my final reports to a company that I work for I suggest that they get a subscription to *2600.* Most of the time they ask me why and I explain that it might help the admins become more aware of flaws etc., but they pass it aside and ignore the suggestion. A few months ago I went in to work on a Saturday, and in the employee break room there were several copies of *2600.* The one that I found most interesting had several articles highlighted throughout. I thought you might find this interesting. By the way, they are buying them at the local Barnes and Noble. I am still pushing them to get a direct subscription but they feel they might get some negative feedback from the government. That I find amusing.

Robert

Food For Thought

Dear *2600:*

I'm here at the Internet Cafe in Sonoma County. They have a T1 Internet access network. Also, let me tell you that these computers are all Compaq computers and they are very nice. You can download music from the net and you can burn music on the main computer. But there is a cost and they have a menu where you can play video games like Star Craft Unreal and others. They however have Microsoft Access. You can use this tool to access files but you can do the same with Internet Explorer.

The Net Cafe has very friendly people. You will not have any problem at all.

If you have a Pocket PC you can hook it up to the computer that you are on and download files.

They have a big selection of computers that you can pick from. This cafe is a very nice place to relax and other things.

However, this cafe has laws that you can't access information. Like hacking or other things you should not do. Please have fun. Please be safe.

Send shirt to [address omitted].

Blair

Perhaps it's time for us to again clarify what constitutes an article. The above is a letter, not an article. It was sent to our letters box so you probably knew it

continued on page 48

DISA, Unix Security, and Reality

by sunpuke

Most people would think that computers used by the Department of Defense would be the most secure systems on the planet. Unfortunately that is not the case, where the vast majority of computers run Microsoft Windows variants. And to secure Windows there is excellent documentation provided by the National Security Agency. But what about Unix? The documentation for securing Unix variants comes from the Defense Information Systems Agency and is a far cry from the NSA's Windows documentation. This is my review of Version 4, Release 3 of the DISA Unix Security Technical Implementation Guide (STIG). If you ever wondered why DoD Unix assets were easy to crack, here is why.

Some people might find this a little harsh, but let's look at how many different operating systems they are trying to give security advice on here:

1. Santa Cruz Operations (SCO) Unix
2. Sun Microsystems Solaris
3. Hewlett-Packard HP-UX
4. International Business Machines AIX
5. RedHat Linux

In addition they cover the installation of Tivoli and MQ Series, all of this in 273 pages. Compare this to the 21 different documents available from the NSA for securing Windows 2000 and Microsoft Enterprise products (ISA Server, Exchange, IIS, Group Policy, Active Directory) and you get the idea that if nothing else the NSA does a better job than DISA. If you want to see for yourself, you can get the document from this site: http://csrc.nist.gov/pcig/cig.html

Unless you have access to .mil or .gov web sites, you cannot get the scripts and additional documentation that DISA provides.

The first thing that becomes apparent is the age of some of the operating systems they are testing. I am all for stability, however that does not mean that (1) I ignore updated operating systems and (2) I believe in security through obscurity. Anyone who has spent significant time examining any operating system knows that vendors make changes on a regular basis and documentation has to be updated to reflect these changes. Unfortunately most of this document is in the "dark ages" when it comes to security and needs significant updates, not only in the methods to achieve better security, but in updating the operating systems the document covers.

C2 and Common Criteria

In the Government you hear a lot of talk about C2 security, and this references the Trusted Computer System Evaluation Criteria (TCSEC) (DoD 5200.28-STD) of 1985. The criteria specified in the TCSEC does not necessarily make your systems more secure, but increases what is audited based on the classification of information that is stored on the systems. The higher the classification, the heavier the auditing requirements become for a system to pass TCSEC. For example, C2 is the minimum level necessary to process Top Secret information. Now why you would want an Unclassified network to audit at that level is beyond me. If you are looking for build methodology, protocols to secure, and other administrative guidance the TCSEC does not have it. The TCSEC was terminated March 11, 1999 by DoD and was replaced with Common Criteria (CC), and the adoption of CC has been slow. The difference between TCSEC and CC is that CC is based on a Target of Evaluation (TOE), and if any changes are made to the system, the evaluation becomes invalid! This is of course if you evaluate each machine individually. This means security (IA) personnel have to determine what a "system" is and how to evaluate it. I will not go into this any farther, but do not expect CC to be used any time in the near future. Basically the administrators are "on their own" when it comes to building systems because guidance is not provided by CC or the DISA STIG other than what is provided in their document. I routinely use Solaris, AIX, and RedHat Linux so I will discuss these operating systems and how the DISA STIG could be improved. This is not an exhaustive list, but some of the more glaring problems I found with the DISA STIG and the methodology.

Solaris

Section 10 starts the discussion of Solaris and the document clearly states, "It is based on Solaris 2.5.1." Solaris 2.5.1 is ancient, and most of the installed Solaris base I have seen are running version 8. I would drop any mention of Solaris before version 7 since that is the minimum OS for 64-bit support and all current Sun hardware is 64-bit. Section 10.1 discusses auditing and how to set it up to DISA standards. One of the many things that is audited is logon and logoff events (lo). Solaris, like almost all operating systems writes its auditing information in a proprietary format that only Solaris tools can read. This means that the process of checking the audit trail for possible intrusions has now become a manual process. The document discusses how to log failed login events by modifying /etc/default/login. The problem is that a user has to fail three times before an event is logged! By enabling SYSLOG_FAILED_LOGINS=0 in /etc/default/login, all failed login attempts are recorded. By doing this, the monitoring of logon and logoff events can be automated because the files are in plain text and can be read by various tools. The coverage of the use of ASET is terrible; ASET can be configured to monitor various directories and files for possible tampering far beyond what is specified. Also the document does not discuss a possible problem in the configuration and use of ASET. If you have built a minimized Solaris machine that does not have NIS installed (packages SUNWnisr, SUNWnisu, SUNWypr, and SUNWypu) running ASET will fail since it cannot find the ypcat command defined in /usr/asset/asetenv. Any reference to ypcat has to be removed before ASET can be run successfully and you are not using NIS. Another area of concern is the discussion of Role Based Access Control (RBAC). The document covers the benefits of RBAC but does not tell you how to configure it, especially if you are running a system without X (there is an article in *Sys Admin* magazine that discusses the use of RBAC without the Solaris Management Console). Finally, the removal of snoop - I do not think it is a good idea to remove a diagnostic tool. Yes, you can capture network traffic with it, but when you need to use it, it is there and should stay. Since it can only be used by root, there should not be a problem unless everybody is root. There is a brief discussion of Trusted Solaris and its limited use in DISA, I like this comment:

"One of the biggest differences between normal UNIX systems and TS is that normal UNIX systems work on the principle of discretionary access control. TS works on the principle of mandatory access control. All users cannot execute all commands or read all files that it looks like they should be able to do."

That is how Mandatory Access Control is supposed to work. It is like setting up an ACL - if it is not specifically authorized it is denied!

AIX

Section 12 discusses IBM's AIX (Advanced Interactive Executive) and the first thing that strikes me is that there is no discussion of AIX 5L! Support for AIX 4.3 ends December 31, 2003 and 5L has been around since October 17, 2000 (AIX 5L 5.0). Furthermore, AIX 5L 5.2 has the installation option of CAPP/EAL4+ security if installed on 64-bit hardware. IBM makes it clear in their documentation (security.pdf) that if you install software or modify the system outside of the parameters used in the evaluation, the EAL4+ certification is invalid. I suppose DISA would have a problem with AIX 5L 5.2 with the EAL4+ features enabled just like they had problems with Trusted Solaris. There is also no mention of the use of the no command to view network settings and modify them for better security (similar to the ndd command in Solaris). Although the STIG mentions Redbooks (www.redbooks.ibm.com), they obviously spent little time there because they could have found several volumes dealing with AIX and security.

Linux

Section 13 discusses Linux and the document states, "It is based on Version 6.2 through 9.0 of Red Hat Linux." Personally I think the authors are a little ambitious in covering seven different versions of RedHat Linux in 19 pages. SuSe Linux was recently given CC EAL2+ certification and this is what DISA had to say about it:

"As of this writing, the only distribution of Linux that has been added to the NIAP Validated Products List for Common Criteria (ISO/IEC 15408) is SuSE Linux Enterprise Server Version 8 (SLES-8). SLES-8 was evaluated against the Common Criteria for IT Security Evaluation Version 2.1 and received an Evaluation Assurance Level (EAL2+) certification. It should be noted the SLES-8 was not evaluated against any of the U.S. Government/NSA sponsored Protection Profiles. Reference (Section 1. Introduction) of this STIG for additional information on NIAP evaluation requirements and product endorsement."

Considering the idea of Common Criteria was to be an international standard, does that mean the EAL4+ rating for AIX 5L 5.2 is any less secure because it was not evaluated against any of the U.S. Government or NSA Protection Profiles? Let's not mention the fact that Security Enhanced Linux (or SEL, an NSA product) is not even mentioned here! If you were trying to build a highly secure Linux system, using SEL allows the administrator to enable Mandatory Access Control and Role Based Access Control features that would make the system very secure. And the comments about Bastille Linux:

"FSO has not subjected The Bastille Hardening System to acceptance testing. It is presently not available from a trusted source. Though Bastille is part of the benchmark project for the Center for Internet Security, it should still be used with caution. If the SA chooses to use the Bastille utilities, the SA should use only the latest version of the product, remove the system from the network before execution, and execute a complete system backup. After use, as a precaution, the SA will verify that the changes selected were implemented and they were the only changes implemented and there were no security vulnerabilities introduced. The SA will perform a self-assessment after using Bastille by running the UNIX scripts and noting deficiencies. The Bastille Hardening System program is available from http://www.bastille-linux.org/."

There are two agencies that are responsible for the evaluation of Open Source software and its use within the Department of Defense: National Security Agency and Defense Information Systems Agency.

So why does DISA not recommend or even mention Security Enhanced Linux? I find it interesting that on one hand they question a CC evaluation because the evaluators did not use U.S. or NSA Protection Profiles, while on the other hand not recommending or mentioning an NSA product. The document does mention the Center for Internet Security and recommends the use of Linux Benchmark, a tool that in my opinion does not go far enough to secure a Linux machine. Specifically the ability for a non-privileged user to reboot the machine by pressing Ctrl-Alt-Del and the ability to use USB devices such as Memory Sticks, amongst other things.

The section concerning Kickstart (13.2.3) I found interesting if for nothing else than to show what I feel is backward thinking on the part of the authors of this document. If DISA were to actually examine Kickstart (as well as JumpStart for Solaris and NIM for AIX), they would find an effective way to deploy machines where configurations would match and could customize the install based on machine function. Sun and IBM are looking to these technologies not only for installation, but also for disaster recovery as well as a management tool (Sun's N1 initiative). It is only a matter of time before RedHat adds similar functionality. All of these use NFS, tftp, and RARP to allow the clients to download the boot image. Like everything else, if enough time was spent researching methods to deploy such servers securely, life for system administrators would be made much easier. Many of the problems associated with Linux are the result of default installations, not just poor system administration. A RedHat Linux box I examined had 853 rpms installed and was supposed to be a DNS server! This is obviously the result of a neophyte system administrator install of Linux.

Section 13.11.1 discusses Linux password aging and what I find interesting here is this statement:

These changes will be applied to /etc/login.defs:

PASS_MAX_DAYS	*90 Maximum days a password is valid*
PASS_MIN_DAYS	*15 Minimum days between password changes*
PASS_WARN_AGE	*10 Days warning before a forced password change*
UID_MIN	*1000 Minimum value for automatic UID selection*
GID_MIN	*100 Min value for automatic GID selection*
PASS_MIN_LEN	*8 Minimum acceptable password length.*

This last line does NOT work in all versions. It is superseded by the PAM module "pam_cracklib". See the pam_cracklib parameter "minlen" for information, or the module on PAM in this document.

The underlined portion of this indicates a problem with PAM, but the authors chose not to specify which version of Linux displays the problems they encountered. The comment in Section 13.4.1indicates serious problems with password checking:

"Linux has very poor native password checking. See the Linux Account Management section for an expansion of this subject."

Again, this should be addressed by what version of PAM this behavior was observed in and how to fix it. They mention the use of passwd+ or npasswd. Both come in source form only and npasswd has not been updated since 1992! In some cases the use of a compiler might not be allowed by some commands. DISA should recommend something that can be installed as an rpm, or provide an rpm for download.

Reality (or life outside of DISA)

The document does not go into any explanation about various build methods and what they can or cannot do for the system administrator. Most of the issues encountered with a Unix machine security wise can be dealt with during or immediately after the installation of the operating system. Virtually all of the machines I have encountered were full operating system installs despite excellent documentation from other sites and books to the contrary. The DISA STIG does not go into sufficient detail on how to actually build a secure machine, nor would I consider a machine built using the STIG as secure.

A recent piece on Slashdot (http://slashdot.org) discussed Information Technology personnel in the military and unfortunately most do not get proper training to perform their jobs. Documentation like the DISA STIG becomes crucial in how military systems are secured. The emphasis cannot be just on auditing. It has to change its focus from a single system mentality to that of a Data Center, where there are numerous systems and that installation might be automated, or hands-off. The authors of the STIG should foster working smarter and not harder.

Specific recommendations to DISA for improving the STIG:

1. Conduct operating system research on current and future operating systems.

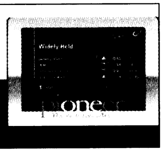
2. If DISA cannot keep up with the latest developments, then recommend security related sites that can such as SecurityFocus (www.securityfocus.com).

3. Recommend products that can improve security without the politics (like not recommending Security Enhanced Linux) because the NSA is in "competition" with DISA for the same job.

4. DISA should write OS specific documentation as opposed to creating one document that tries to cover everything. Tivoli and MQ Series should have their own unique documentation.

5. If DISA is going to report a problem with an operating system, they should also provide a relevant fix that can work in all situations or provide the fix themselves.

Hacking the "Captivate" NETWORK



by Darlok

No doubt many of you have seen those fancy computer screens mounted in elevators in office buildings in major cities like New York, Chicago, and Boston. They provide news, sports, weather, advertising, and other information to the occupants as they enjoy the ride. Well, I was recently able to do some poking around with the Captivate network in my building. Once I figured out that they were actually wireless devices residing on an 802.11b network I broke out my wireless hacking tools and went to work.

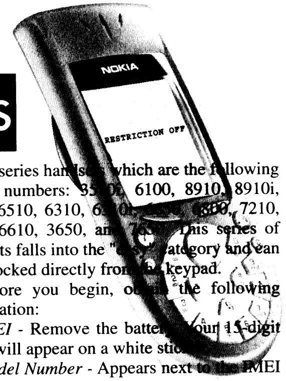
In my case, the wireless network did not have Wired Equivalent Privacy (WEP) enabled, so it was open. However, I couldn't obtain an IP address, so I figured either DHCP wasn't running or the network was configured to disallow new clients from associating with an access point and getting on the network. It turned out that the latter was true. How did I know? After using Kismet to capture IP and MAC addresses, I did some MAC spoofing. Once on, I typed the IP addresses of one of the APs into my browser and got the administration page for a Cisco

Aironet 4800E. To my (mild) surprise, it was not password-protected, so I was able to basically do whatever I wanted.

The main thing I wanted to do was configure it to allow my machine to associate. I accomplished this by navigating to the "Association" page and changing the "Allow automatic table additions" option from "off" to "on." I was now able to freely associate with this access point without having to spoof a MAC addy. I then performed some network discovery and OS fingerprinting to see what I could see.

I discovered that the screens mounted in the elevators are actually wireless PDA-type devices running WindowsCE and that they have Telnet open. I also found a lone Windows 2000 server which, according to my packet sniffer, was broadcasting the images to the elevator screens every few seconds. As much as I wanted to, I suppressed the urge to attempt to inject my own images. And yes, I also set the "Allow automatic table additions" option back to "off." Anyhow, I hope this proves interesting for some of you wireless hackers out there.

Unlocking GSM Handsets



by The Prophet

Ever wonder why most cellular carriers gladly give you a "free" phone? It's probably because they have "locked" the phone to their network so you can't use it with any other carrier. At least, that's the theory. In practice, you can often unlock your handset and use it with another carrier.

Why should you care about unlocking your handset?

- Perhaps your phone broke and the replacement handset you bought on eBay was sold by another carrier - so with your SIM, all it does is display "network barred."

- You might want to try out a friend's phone and see whether it's right for you... but you have AT&T and he has T-Mobile.

- What if you hate your carrier but you love your phone and you want to switch it to another provider? Too bad if it's a locked handset because you can't do it... or can you?

- Maybe you just don't want your cellular phone company telling you which carriers you're allowed to use.

Whatever the reason, it's your phone. You paid for it, and whether or not your carrier wants you to do so, it's your right to unlock it. Best of all, it's still legal (in most areas - for specific legal advice concerning your situation, always consult an attorney).

Depending on the particular model of GSM handset you have, it can be anywhere from really easy to almost impossible to unlock it. This article will focus on the Nokia DCT4 series handsets which are the following model numbers: 3510i, 6100, 8910, 8910i, 8310, 6510, 6310, 6310i, [illegible], 6800, 7210, 7250, 6610, 3650, and 7650. This series of handsets falls into the "easy" category and can be unlocked directly from the keypad.

Before you begin, obtain the following information:

IMEI - Remove the battery. Your 15-digit IMEI will appear on a white sticker.

Model Number - Appears next to the IMEI sticker.

Network Provider Code - The numerical identifier of your GSM provider. Some common network provider codes are as follows:

31038: AT&T Wireless
31015: Cingular (east coast)
31017: Cingular (west coast)
31016: T-Mobile (east coast)
31026: T-Mobile (west coast)
31031: T-Mobile (Florida)

Note: There can be some trial-and-error associated with the network provider code since these change frequently. If you're not sure of the network provider code for your carrier, be sure to research and obtain the correct code before attempting to unlock your phone. You are only allowed five unlock attempts!

Next, download and install a DCT4 calculator. A good one is located at the following URL: http://www.uniquesw.com. If this page no longer exists, search the Web for "DCT4 calculator" and you should find one.

In the DCT4 calculator, type your IMEI and network provider code (some DCT4 calculators refer to this as an "operator code"). Additionally, select the type of phone you have. Double-check that everything is correct and calculate your unlock codes. A result similar to the following example will be displayed:

#pw+349456762705141+1# - lock 1 (MCC+MNC)
#pw+126044647431732+2# - lock 2 (GID1)
#pw+343066263131352+3# - lock 3 (GID2)
#pw+259575473756767+4# - lock 4 (MSIN)
#pw+393436415125521+5# - Unlocks lock types 1 and 2
#pw+192464412045251+6# - Unlocks lock types 1, 2, and 3
#pw+799620614767516+7# - Master unlock - removes all locks.

The first four codes displayed are lock codes. The final three codes are unlock codes. You will probably want to use the master unlock code (ending in 7#) because it unlocks everything.

All right, you're ready to go! Take the SIM card out of your phone and then power it on. When your phone displays "Insert SIM," enter the unlock code at the bottom of the list (ending in 7#), exactly as shown in the calculator:

To enter the "+" character, press the "*" key twice.
To enter the "p" character, press the "*" key three times.
To enter the "w" character press the "*" key four times.

Your phone should pause briefly and then display a "Restriction Off" message. Congratulations! Your Nokia GSM handset is now unlocked and will accept SIM cards from any carrier.

Troubleshooting

If things don't work as expected, confirm that you didn't make any data entry errors and then try again. If you still have trouble, you may want to review the references and message boards below. You only get five tries to get this right before your phone locks you out of the service menu, so if you don't know what you're doing, ask someone who does! There are plenty of GSM hackers out there who will be glad to help.

References

DCT4 Calculator: http://www.uniquesw.com
Nokia unlocking FAQ:
http://gsmsearch.com/faq/nokiaflasher.html
Nokia unlocking message boards:
http://www.nokiafree.org
General wireless message boards:
http://www.howardforums.com,
http://www.wirelessadvisor.com

Appendix: North America PCS Technologies

In North America, there are four widely available digital (often marketed as "PCS") technologies in use, along with the legacy (and still operational) AMPS analog cellular network. While the above article is about unlocking GSM phones, CDMA phones can also be "locked" to a particular carrier through a method called Master Subsidy Lock (MSL).

What follows is a list of PCS technologies:

CDMA: Used primarily by Verizon, Alltel, US Cellular, Qwest, and Sprint PCS, CDMA service is operated on both the 800MHz cellular and 1900MHz PCS frequencies. This technology supports both voice and data applications. There are two variants of CDMA in wide use. The newer version, 1xRTT, allows for data speeds of 144Kbps, has better call quality, and offers greater spectral efficiency for voice applications. The older version, IS-95, supports data speeds of up to 14.4Kbps and uses a less efficient voice codec.

TDMA: Used primarily by AT&T and Cingular, TDMA is a legacy technology that supports only voice applications. It operates only in the 800MHz cellular frequencies and is being phased out by both carriers in favor of GSM.

iDEN: Available only from Nextel in the US and Telus MIKE in Canada. This is a proprietary Motorola technology that supports voice, data, and "walkie-talkie" features. It operates on two-way radio frequencies in the 800MHz range.

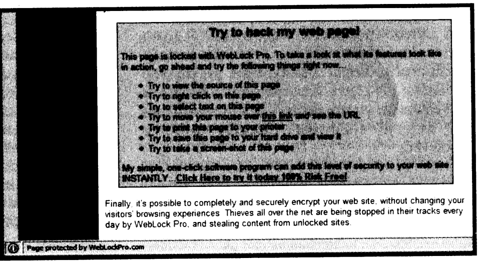
GSM: Available from AT&T, Cingular, and T-Mobile, among other carriers. Primarily operates in the 1900MHz "PCS" frequencies but many carriers are beginning to offer service in the former 850MHz TDMA spectrum. While widely considered to offer better voice quality than CDMA, GSM is much less spectrally efficient. Additionally, GSM does not offer "soft handoffs" like CDMA, making it more prone to drop calls. Data services, called GPRS, are circuit-switched and operate up to 56Kbps.

Acknowledgments

UniqueSW - for their excellent - and free - DCT4 calculator.

Nokiaguru - for the Nokia unlocking FAQ, without which I'd never have used the above calculator successfully.

Unlocking WebLock Pro



Try to hack my web page!

This page is locked with WebLock Pro. To take a look at what its features look like in action, go ahead and try the following things right now...

- Try to view the source of this page
- Try to right click on this page
- Try to select text on this page
- Try to move your mouse over this link and see the URL
- Try to print this page to your printer
- Try to save this page to your hard drive and view it
- Try to take a screen-shot of this page

My simple, one-click software program can add this level of security to your web site INSTANTLY... Click Here to try it today 100% Risk Free!

Finally, it's possible to completely and securely encrypt your web site, without changing your visitors' browsing experiences. Thieves all over the net are being stopped in their tracks every day by WebLock Pro, and stealing content from unlocked sites.

Page protected by WebLockPro.com

by Schnarf

A while ago I was reading some forums and someone posted a link to WebLock Pro (http://www.weblockpro.com/). The website claims "Breakthrough technology finally puts an end to web site theft..." The author, Mike Chen, sells this software for $49.95. So, to put it simply, he posted two blocks of unescaped code and the decrypted _c variable, and encouraged anyone else to "give it a try." I did, and these are my results.

Before posting the Perl script, I'm going to explain how it works. I'll use the example of http://www.weblockpro.com/home.php. First, go to view page source. All you see should be "<Page protected by WebLockPro.com>". When I first saw this, followed by whitespace, I was curious whether he used some sort of whitespace-only encoding. However, that's not the case. Scroll down, then a bit to the right. There's a block of javascript. First, there's an eval(unescape("%77%69...")). This is simple to decode. It results in:

window.status="Page protected by WebLockPro.com";_dw=document.write;document.write=null;

Next is a variable called _c, which is followed by a second block of escaped code which is evaluated. When unescaped, it comes out as:

```
function _x(s) {
     s=unescape(s);
     t=Array();
     t[0]="";
     j=0;
     for (i = 0; i < s.length; i++) {
          t[j] += String.fromCharCode(s.charCodeAt(i) + (i%2==0 ? 1 : -1));
          if((i+1)%300==0) {
               j++;
               t[j]="";
          }
     }
     document.write=_dw;
     u="";
     for(i=0; i<t.length; i++) {
          u+=t[i];
     }
     document.write(u);
     u="";
     t=Array();
     _dw=document.write;
     document.write=null;
}
```

This function is referenced after the second block of escaped code. _x is the function which actually decrypts the data and writes it to the document. Looking at the first block of code and then this again, there is a bit of trickery: document.write is saved to _dw, then null is assigned to document.write, causing document.write not to work. In order to write data, _dw is assigned back to document.write, the function is used, then null is again assigned to it. We can see on the last line the call to _x, the parameter of which is the actual encrypted page data. Really, in the entire process of figuring this out, there was no cracking of any code, merely unescaping or otherwise unobfuscating one block of code to understand the next. Now, my only task was to convert the javascript function to Perl, which was no feat. The culmination of this work resulted in the following Perl script:

```
#!/usr/bin/perl

# The DMCA says: "a person who has lawfully obtained the right to use a copy of a
#computer program may circumvent a technological measure that effectively controls
#access to a particular portion of that program for the sole purpose of identifying
#and analyzing those elements of the program that are necessary to achieve interop
#erability of an independently created computer program with other programs . . . to
#the extent that any such acts of identification and analysis do not constitute
#infringement under this title."
#This script is, of course, only to ensure interoperability with non-javascript-
#compatible browsers.

# Open the file
open (F, $ARGV[0]) or die "Could not open $ARGV[0] for reading: $!";
@raw = <F>;
close (F);
$page = join ("\n", @raw);

# Get the data to decrypt
$data = getData ($page);
# Now decode that data
$final = decode ($data);
# Print it to STDOUT
print $final;

# This just grabs the parameter to _x
sub getData {
     my $page = shift;

     my $start = index ($page, '_x("');
     if ($start == -1) {
          die ('Could not locate start of raw data!');
     }
     my $end = index ($page, '");</script>', $start + 4);
     if ($end == -1) {
          die ('Could not locate end of raw data!');
     }
     $start += 4;

     return substr ($page, $start, $end - $start);
}

# This is just _x converted to perl
sub decode {
     my $s = shift;

     $s = unescape ($s);
     my @t = ();
     my $j = 0;

     my $i;
     for ($i = 0; $i < length ($s); $i++) {
          $t[$j] .= chr (ord(substr ($s, $i, 1)) + ($i % 2 == 0 ? 1 : -1));
          if (($i + 1) % 300 == 0) {
               $j++;
               $t[$j] = '';
          }
     }

     my $u = '';
     for ($i = 0; $i < $#t ; $i++) {
          $u .= $t[$i];
     }

     return $u;
}

sub unescape {
     my $str = shift;

     $str =~ s/%([a-fA-F0-9]{2})/chr(hex($1))/ge;
     return ($str);
}
```

This perl script takes one argument: the filename containing the data. For example:

```
$ wget http://www.weblockpro.com/home.php
$ ./decode.pl home.php > fyad.html
```

The decrypted page will now be in "fyad.html."

Other Stuff

There is a method of rich format copy/pasting to get around the obfuscation. In Mozilla, "Select all/copy, fire up composer, paste, add base href (too lazy to grab all the images), save." The only downside is that it doesn't copy javascript or other non-visible elements.

It's not hard to make this Perl script into a CGI Proxy.

Where does this stand with the DMCA? Check the comments of my Perl script.

Thanks to: R1CH (http://www.r1ch.net/) and Xenomorph (http://www.xenomorph.net).

Shout outs: #cpp, snafu, redhackt, mish, madcow, zeet, and g0thm0g.

continued from page 39

wasn't an article. Articles are usually much longer and go into significant detail. Telling us these very general facts about this cafe is not exactly breaking news. And people who write short letters to us don't get the free subscription and t-shirts that authors of articles get. If you look at the number of letters we print you can probably see why this is.

Dear *2600:*

On my routine sweep of Internet technology websites, I came across Eric S. Raymond's "How to be a Hacker" page, linked to by another document. Amused, I read and read... and read some more, as it's a very long document. I agreed with many things he said, surprisingly, including the fact that you hack to learn, not learn to hack, and that programming is hacking while breaking into websites is not. One thing he said, however, disturbed me. He stated that aliases (such as mine, Code_Dark, or anyone else I know that's involved with *2600)* promote cracking and are telltale signs of false and wannabe hackers. What do you guys think about this? Aliases are a must in an age with no anonymity! Do you think that none of us are hackers, or that this "revered geek" is simply wrong?

Code Dark

It's one view and obviously we don't agree with that part of it. Nor do we buy into that whole hacker/cracker thing. But there are a lot of simplistic tasks involving computers that are incorrectly referred to as hacking which require no skill at all - many instances of people breaking into websites require nothing more complex than running a script. Others, however, do require hacking skill. It's tempting to reject the entire process if we don't like the outcome. But it's more productive to try and reach those people with hacker skills so they use them in a positive way.

Dear *2600:*

I went to the cnn.com website and did a search for articles containing "hackers" and then went to cbc.ca and ran the same search and was amazed at how many more articles showed up at CNN as opposed to CBC. Is there more hacking in the US than in Canada? Or does Canada just cover it up or does the US make it up?

nameless

If you read the actual stories you'd quickly see how few of them actually had anything to do with hacking. But the word "hacker" gets people to read the story.

Dear *2600:*

I noticed one thing I have never seen in any of your magazines, and that is about Product Keys for Windows 98. Maybe there was an article and I missed it, but just in case, here is a little piece of info that I recently noted while checking out the system registry and data files. There is a file called system.dat, normally located right in the Windows directory. If you edit or open the file with wordpad, you can search through it to find the product key. The easiest way to do this is to go to edit and click on "find" in the search box, enter "ProductKey", and then click "find next." This is helpful if you lost your manual or the Product Key for your Windows Installation CD. Or, use your imagination....

SoftwarePir@te

Dear *2600:*

Wandering around Crate & Barrel the other day, I came upon one of those touch-screen gift registry terminals they have around the store. With nothing better to do, I tapped the bottom left and top right areas of the screen twice and a password prompt was displayed. Above the password box, it said: "Terminal 405b." I punched in 405 for the password and a new menu came up. This menu is mainly used for docking and uploading the price guns into the computer system, but there were also gift registry terminal options, like the ability to render the station completely useless by deactivating the main menu buttons. I didn't have enough time to completely explore the submenus, but it was quite interesting.

Jon

Dear *2600:*

Most government agencies provide a listing of their field offices on their websites. I have found no such listings for The Department of Homeland Security on their website, dhs.gov. I went looking for listings one day when I received an order on my website from someone claiming to represent DHS. We occasionally sell items to several government agencies (some past customers include the EPA, FBI, and ATF). I assumed it was a prank (I was sure that *2600* or one of its readers was behind it too), and to combat this I usually do a Google search for the provided shipping address to see if it is associated with a government building. Or I check the agency's website to see if it is a field office.

Since they don't seem to provide the listings, one can only assume that they don't want us to know where their field offices are, which strikes me as very bizarre. Google gave me no hits for DHS. So I searched further. The address they provided to us for shipping was 610 South Canal Street, Suite 1100 in Chicago, IL. After doing some searching around, I found out that this building houses The Chicago Regional Computer Forensics Laboratory. But there is no mention on the CRCFL's website (chicagorcfl.org) of the DHS setting up shop there (or anywhere else - the DHS website only gives the address of their Washington DC headquarters).

So it's obvious to me that they don't want anyone knowing they have an office set up there. It's odd that DHS is setting up hidden offices in various government buildings. One can only wonder how long it will be before your local Quickie Mart has a few DHS operatives working out of a back room. So, if you notice anyone suspicious, be a good American and report them to your friendly, local DHS office by calling 312-983-9300. This number is answered by US Customs.

Anonymous

We realize they're probably just busy. Redefining what a country the size of the United States stands for is probably taking the vast majority of their time. We'd be happy to lend a hand by printing a full directory of where they're setting up shop as soon as we get the info.

Info Needed

Dear *2600:*

Somewhere around 1984-86 while doing some dialing I ran across a number that answered with a recording of someone reading a series of numbers. I seem to remember that it was known of in the community's collective mind but I don't know what it was. Has anyone heard about this? What is/was it?

Mike

You waited until now to ask? If you could give us a bit more detail on what numbers were being read off, pattern, etc., we might be able to help track this down. If any readers remember, please write in.

Dear *2600:*

I enjoyed the article about ripping a DVD to a Pocket PC PDA, but unfortunately I use a Visor Prism (color screen, Palm OS). I think all I need is a media player for Palm OS, but I can't seem to find one. If anyone has a guide to DVD viewing for the Palm OS, I'd love to see it in *2600.*

Scott

Dear *2600:*

This question primarily goes out to my fellow *2600* readers. Has anyone ever probed Amtrak's computer system on any level? Their horrible job performance must have pushed someone to investigate them in some way. Also, is there any information out there about their Quik Ticket kiosks set up near the Amtrak ticket booths? I would be infinitely grateful if someone could shed light on this topic.

Uncle Dust

Dear *2600:*

Supposedly at some point in the early 1980's, a misconfiguration in AT&T's computers caused all long distance calls made during the day to be charged at the night rate, and vice versa. This state of affairs continued, so the story goes, for two weeks before being corrected.

Have you heard about this? Is the story true? Where can I read authentic details?

Elvis Carter-Abbot

It sounds a bit like folklore to us. If such a thing had happened back then when phone rates were a lot more expensive and meaningful, it certainly would have been front page news.

Ominous Developments

Dear *2600:*

TIA is alive. While I know of no means of petabyte storage, the data handling and visualization is well past beta version. It seems that like all things, this has been in the works for quite awhile. Starlite (http://starlight.pnl.gov/) is the means to this data processing along with software from DataViz that intelligently places xml tags on things like names, events, places, etc. I have seen a pitch for this software and have every inclination to call it godlike in capability; unparalleled in data mining. It makes Google its bitch. That said, look around. The data gathering agents are in place. WeatherBug (aptly named) sends info to Homeland Security. They never say what that info is. Check the language used in the privacy statement, you'll see what I mean. Add to that the new legality of the monitoring of packet switched networks and the current voice recognition tech and you've got yourself a big ol' TIA. Unbelievable technology. My challenge to all the readers is to do a thorough article on Starlite and one on the use of WeatherBug to gather "other" data (sniff your packets) as I have not the time. Good luck.

czarandom

Just when you thought it was safe to go outside.

Dear *2600:*

I wanted to make you aware of how much we are going into a spiral with the paranoia that's out there in this country.

I work as a network engineer for a telecom company in the DC Metro area and have made a nice living from it during the past years. This past October when the weather started getting cold my heating system died. So I called my local heating guys (FW Harris) that I've used in the past. So two heating guys showed up at my door, inspected my heating system, gave me an estimate, and left.

A week later I was visited by local rookie FBI agents telling me they had a report that I had a lot of computer equipment in my house and maps. This just threw me for a loop, so being of sound and educated mind I showed the rookie FBI agents what my computer equipment consisted of. In my basement I have a home office setup .On one side I have my 21 inch monitor and a PC that I built myself and on the other side my roommate has his 21 inch monitor and PC with a multipurpose fax machine hooked up. When the rookie FBI agents saw how much equipment I had they were like, "Huh, that's all you have?"

Then they asked me about the maps. It struck me that when I was getting the estimate from my friendly neighborhood heating guys in my kitchen I had a small pocket DC metro map on the kitchen bulletin board and that's what they were referring to as "maps." After this I knew the heating guys called the TIPS line on me because I am of Middle Eastern descent even though I was born and raised in America and also because the two heating guys saw my computers and a DC metro map and took that as a threat for some reason. After the rookie FBI agents apologized and said that they were only doing their job following up on leads that they receive, I called the heating company and gave them a piece of my mind. So I advise your readers to not use FW Harris in the DC metro area. If this can happen to me, don't think it can't happen to you.

Iz

Annoying Problems

Dear *2600:*

Point me in the right direction for some software programs. The reason I am asking is that I am having some trouble with a person in a newsgroup that is "spoofing" me. I have actually been able to take the information back to the ISP, but when I make a complaint to the ISP they ignore it even with complete headers of the messages.

As it stands I am being hit with threats from other posters about posts made from this person "spoofing" me and them thinking that it is me doing it. I can live with this if I can get this person to stop doing this, but again the ISP refuses to do anything.

Now I have seen some people that are able to actually get the names and addresses of people through their posts and this is what I would like to be able to do. No, I will not use this to attack this person, as all I want to do is send them an e-mail through an anonymous remailer just to warn them I know who they are and what they are doing and ask them to cease. I know this sounds "farfetched" but I really have no desire to harm anyone. I just want this person to cease.

I have asked some questions about this in chat rooms and even the alt.binaries.2600 newsgroup, only to be laughed at and be told that if I asked such a stupid question again, my personal information would be posted all over the net. Personally I don't see what I actually did wrong. Nor why I was being treated like I just demanded the keys to the Internet backbone. So far what I have learned about tracing an ISP I learned at geektools.com and by using smartwhosis.

Now you see why I would like to know how to actually get the name and address of this person so I can get him to stop. Heck, I would even send you the headers if you would give me this information just to prove to you that I am not out to hurt anyone.

A little help here please? Some names of the programs that do what I ask would be great as I could locate them on my own.

Thanks guys, your magazine is great!

Daniel

The Internet is comprised of all kinds of people ranging from morons to geniuses. And there are very few among these who don't enjoy watching reactions when certain personalities clash. When you ask for help, you will invariably get mocked by people who either want to provoke more of a reaction or who simply like to be obnoxious. Many times this turns the original poster into an hysterical lunatic and their progression into eventual institutionalization becomes a source of entertainment all around the globe. You can avoid all of this by not taking it all too seriously or, at the very least, not appearing to take it too seriously. If you find out about a fake post that went out somewhere, post as yourself and make it clear that this wasn't you and you'd appreciate it if someone would help you figure out who it actually was. Depending on software and methods used, this is usually not very difficult and someone in all likelihood will step forward. If they don't, there's no point in making an issue of it. An ISP has better things to do than get involved in something relatively minor like fake postings. But there are plenty of people out there who will lend a hand if you don't come off as a nut. And if you show no outward signs of being upset at what's going on, whoever is behind it will eventually get bored since there's no longer any entertainment value.

Dear ***2600:***

I don't read your magazine, but my brother's letters got published twice. Please stop.

Erik

He told us you'd say that.

Dear ***2600:***

Imagine you type your name into a web browser and a picture of a dead fetus pops up in your face. Take a look at www.zacharysmith.com. This is my name, and it is being abused. What can I do? I have already tried the friendly approach; any ideas would be more than appreciated.

zs

There's not a whole lot you can do legally if they aren't actually defaming you personally. But you might try being a little creative and registering the name of a vocal pro-lifer and pointing the domain at something they truly detest. Then perhaps a trade could be organized.

Dear ***2600:***

At the newsstand where I buy my issues of *2600*, they cover up the word "Hacker" in "The Hacker Quarterly" with a $5.50 price tag. After buying two years worth of issues, I have noticed that the newsstand never deviates from this. I wanted to know if other readers experience something like this from their respective newsstands and if so, if it is an indication of the negative connotation that has been placed on the work "Hacker" or just a fluke.

sandman10_99

We would bet it's most likely the same person doing the same job for so long that they know of no other way of doing it.

Dear ***2600:***

I am being stalked by a computer! A computer driven by a cowardly poor excuse of a man. When I lived in the apartment above his, he used sound to drive me crazy and vibration to make me go to the bathroom. He would go in his bathroom when I was in mine and tap some signal letting me know he was listening and at a later level he would leave feces at my apartment door.

This Ahole took all my messages off my message machine, of which in my time there I had three. He probably listened to my phone calls. There were always clicks in my walls when using my latest phone/message system. He changed my voice messages and took my messages off. He got into my TV and I cannot use my menu screen. He took the caption off and lowered my sound among other things. I don't care how he does this. He stays up all night with no lights on and works on his computer. I moved - that was great! No. Somehow he's here doing the same things. After two months, he is still a pain in my ass and causing me to be very sick.

Can I stop this, short of having his fingers cut off? How do I do this?

Lily

We assume you're asking us how to stop this and not how to have his fingers cut off. We strongly suspect you're the victim of a rather large practical joke and/or an overactive imagination. We get many such letters and they all go along pretty much the same lines. Someone is terrified of a person who can do anything to their technology and who is unstoppable. It's a great plotline for a movie but in real life it's not so simple. But what is simple is getting someone to believe that such all-encompassing magic is possible. Once that's achieved, you are completely under the person's control because everything bad that happens will then be blamed on this person, thus making him more powerful with each technological misfortune. The symptoms you describe (apart from the feces and pipe tapping) are all quite common in everyday life. His being on a computer all night is almost certainly irrelevant to your problems. And it's likely he will stop whatever provocations are aimed at you once you stop reacting as if he were evil incarnate. Such a perception tends to inspire many such performances.

Appreciation

Dear ***2600:***

Being an avid reader I love page 33. And in this last issue there was what looked like a math problem. So in my curious way I added, subtracted, and divided. Sure enough, 33.

You guys kill me. And thanks for the great magazine.

ReDLiNe135

You're welcome. But those numbers weren't just normal numbers. It's actually a bit scary when you think about it.

Dear ***2600:***

I don't know if this is the proper place to write to, but I just got all my H2K2 VCD's and I must say I am *impressed!* They are informative and well worth the minuscule dollars you all charge for them. So, just a big thank you from a loyal subscriber and fan.

Tarball Gunzip

We've gotten a lot of good response to these. The real credit of course belongs to the people at H2K2 who put on such great panels that remain interesting to this day. Let's hope we do as well at the next conference this July.

Reader Advice

Dear ***2600:***

I've been reading *2600* for several months now. I first started reading it after a recommendation from a tech friend in my office. His comment on it: "I know of three places in this area that sell it. I always pay cash and I never buy from the same place twice in a row."

The way I figure it, this sounds like good advice to me. Our mutual Uncle Sam seems to realize that since he can't stop or kill the hacker movement, since it is for the most part a freelance phenomenon, he had better track it as best he can.

I'd advise those buying *2600* to be careful in the manner in which they purchase it, unless they want to end up on a Homeland Security watch list. I would wager subscriptions, directly from the magazine and away from third party interests like Amazon.com, to be a safe bet for anonymity, but for myself I'm not taking any chances.

Stone Wolf

If you really believe that this kind of surveillance is ongoing, then the best way to battle it is for as many people as possible to jam up the lists. Our engaging in subterfuge simply strengthens the hand of those who want us to hide and be perceived as criminals. This is why we have our meetings in open places, why we have the magazine available to anyone in the world, and why we don't shut anyone out who expresses a desire to learn and share information.

Dear ***2600:***

I got an e-mail the other day telling me that my e-mail account would be deleted if I didn't forward the e-mail to everyone I knew. You may have also received this notice. I just wanted you to know, it is entirely fake. Don't send it, just delete it.

Chris

Since it's standard practice to send e-mail to everyone you know in order to keep your account from being turned off, a lot of people must have fallen for this one. Thanks for waking us up.

Dear ***2600:***

In the last issue, I noticed that there were a lot of letters about learning to hack, and I can completely empathize. When I first came onto the scene, I was greeted by rude know-it-all's who weren't willing to teach (whether they actually knew anything is another discussion). So I did the best I could with what I had available to me. I started reading books about computers. I took computer related classes. I made friends at school who were in the same boat I was in. When I made it to university, I studied computer science. That helped a lot. By the time I went to graduate school, I was reading hacking texts off the net and saying to myself, "I already know this." Now I'm out of graduate school and deeply in debt from student loans, but I can say with confidence that I'm good at what I do. I can hack. So there it is, the beginner's guide to how to hack. Study hard, be diligent, and always be creative. Lather, rinse, repeat.

crypto

Stories of Insecurity

Dear ***2600:***

I have been a reader of your publication for about a year, and this is my first attempt at any sort of letter. I simply wanted to share my story with fellow hackers.

I am a 25 year old systems admin/programmer/deskside support/hacker, that works for a rather large insurance company. I am deeply involved with my carrier which results in my need for a laptop (company issued). I also have a wireless network at home (I know, I know...) simply because the freedom of sitting on the couch and creating user IDs is wonderful. I have taken all the wireless precautions that I have read about, so I feel relatively safe using my wireless setup. I change DHCP users to 2 and back to 1 when I remove my laptop. Changed my default IP, checked the logs, changed my password, and so on and so forth.

Like every day I was in a rush to get to work so I forgot to remove my wireless card and went out the door. I sat at my desk, powered on my laptop, grabbed a cup of coffee, and returned to my desk, only to notice my wireless nic had a link. I know my network inside and out and I have no wireless equipment in my server room or anywhere in the building for that matter. Like any self respecting hacker I began to survey the network in which I was bound. Beginning with finding out what my IP was. 192.168.1.x. I couldn't believe the luck. Opened IE and 192.168.1.1 was - you guessed it - the router. Username: [blank] Password: Admin. I was in. Once I compiled a list of all available IP's I ran tracert on the IP's to get the computer name, then simply entered the name in the run box preceded with \\machinename\sharename.

Guess what? Every computer on this "network" was *wide* open, no passwords on shares, etc. I looked around in a couple of machines, something I probably shouldn't have done, but I needed to see if I could gain more info about the network I was now married to. I quickly found something named invoices.doc. I opened it and there in front of me was a list of 16 names, along with account numbers, social security numbers, credit card numbers, everything that should not be in a Word document. I quickly closed this and I ended my searching after I found a machine called "scott." (This entire time I was creating a spreadsheet of all open machines accompanied with IP addresses and everything a sys admin would want.) Now I decided to take Scott's machine, take screen shots, and print them, for proof that I was in the network without printing the list of account numbers.

After all the research had been completed, I decided to embark upon my quest to find the owner of this network to inform him of his /her new project for the day. I work in a four story office building. Floors 1, 3, and 4 belong to my company. Floor 2 belongs to another company. I started with the current occupants of the 2nd floor only to find out they barely even knew what a computer was, let alone a network. I was informed that nothing was done locally - they had to call a hotline if their computers were "messed up." I told them that I thought they had an issue and needed to speak with someone. I eventually came to the conclusion they had no wireless equipment in the building. There is another clone of my building within spitting distance of my office so I decided to contact the building owner to find out if I could match a name with any of the names I found in the network. They were quick to provide me with information, even without me clearly stating my purpose. Needless to say I was amazed. The name of the "computer guy" was Scott. Was I shocked? *No.*

Here is where my inner voice stopped me, because what I did to gain this information could be considered a terrorist act and I didn't want to be labeled as such. So I had a lengthy internal battle over what to do and eventually decided to march over there and hand Scott basically his walking papers if his boss found out. So I went over and asked for Scott. I explained to him what I found and he immediately went and grabbed the president of the company who just so happened to be touring the building that day. I repeated what I had explained previously to Scott and told them it was very simple to prevent. I also provided both of them with all of my hard work, aka "proof" and explained about the invoices.doc. I was picking chins up off the floor because what I had found was medical patient data. This company turned out to be a collection agency for hospitals. I come from a medical background. My father, grandfather, and three uncles are doctors. So I know plenty about the HIPAA regulations (http://www.hipaa.org/). I thought I was going to jail for sure, but these two individuals were very interested in learning more. A long winded adult discussion ensued about security and what Scotty boy needed to do to fix it. I was provided with a card from the president and they have contacted me a few times just to thank me or say hi. A very happy ending to something that could have had disastrous results.

Although this was obviously the desired outcome, it was pure luck that I ran into two people that were eager to learn how to remedy the issue and how to take future security measures. I wouldn't have figured a company that has that amount of government issued regulations would have had such a poor system in place. I mean this guy had a Linksys BEFW11S4 router running a company. Enough said.

Cory K.

There's no question you did the right thing here. We hope others aren't intimidated by the potential paranoia and stupidity they may be met with. The more success stories out there, the easier it will be to show how such security holes and the people who find them should be dealt with.

Dear *2600*:

I had heard that the Mac OS X version of MS Office doesn't require a registration code and it includes an automatic utility to restore missing system files, meaning all one has to do to pirate it is copy the whole Office folder out of the Applications directory. The Office folder is over 200 MB in size, but that's no problem thanks to the Apple iPod, which will mount automatically as an external hard drive on any Mac by plugging it into the FireWire port which all recent Apple computers have.

As an experiment, I decided to try this out at my college's computer lab. Not only was I able to pirate Microsoft Office X with a single drag-and-drop, but I was also able to pirate the entire Macromedia product line. The Macromedia products did require a registration code, but it was easily available by bringing up the "About" dialogue in each application and copying the codes to a text file, which also went to my iPod. Investigation on my home computer showed that the code in the "About" dialogue was indeed the same one required to register a new installation. The only products I wasn't able to get using this method were the Adobe product line, which display all but the last four characters of their registration code in the "About" dialogue. All in all, I found it was possible to pirate hundreds of dollars worth of software from my college's computer lab in under five minutes. This same method would probably work as well anywhere that a naive person has set up an unsupervised Mac OS X computer for public use, such as CompUSA.

The irony of this situation is that my university has all sorts of security software installed on their Windows PCs, but their Macs are in out-of-the-box default settings. Presumably they feel that the Macintosh platform is unpopular enough that no one will do anything bad on it. It goes to show once again that obscurity is not security.

Of course I erased all the software once I got home, because software piracy is illegal.

Zardoz

HOLES in Windows 2003 Server

by Joseph B. Zekany

This article is written to help all of the Windows system administrators who are thinking of deploying Windows 2003 server. Along with all of the new improvements Microsoft has made with this release of Windows, some things stay the same. Microsoft has made some improvements in security for those administrators using the setup manager for remote system deployment. Or did they?

Setup Manager is found in the deploy.cab file which is in the support/tools folder on the Windows 2003 server CD. Just extract the Setup Manager program by right clicking on deploy.cab and selecting open, then copy the files where you want them.

Introduction

The Setup Manager program is used to create an unattended answer file used with remote installation service to deploy Windows XP professional desktops and .NET servers throughout enterprise networks. When you run setupmgr.exe the program starts an easy to follow wizard that asks you for all of the information needed to install Windows XP Professional or Windows 2003 server and puts this information in a file with a .sif extension. The default name is remboot.sif. This file will be used by remote installation service after the client has downloaded all of the files needed to install Windows. When the setup begins it will use the remboot.sif file associated with the Windows image stored on the server and provides the answers you gave the setup wizard. This can make life for a system administrator a lot easier - or a big hassle.

The remboot.sif file is a simple text file that is similar to the win.ini and system.ini files in previous versions of Windows. It has several blocks of data broken down into the following sections: [Data], [SetupData], [Unattended], [GuiUnattended], [UserData], [Display], [Setupmgr], [Identification], [Networking], [RemoteInstall], and [OSChooser].

In the version of setup manager that came with Windows 2000 Server, the block [GuiUnattended] had the following directives: AdminPassword, OEMSkipRegional, TimeZone, and OemSkipWelcome. The AdminPassword directive is used to set the local Administrator password on the machine being setup. This password is stored in clear text in the file. This file is stored in a shared directory that can be read by everybody, leaving the network wide open to even low-level users who are sharp enough to search for it.

The Change

Microsoft has changed the AdminPassword directive in the Setup Manager that ships with Windows 2003 server to include an option to encrypt the Administrator password. This is a great idea. Or is it?

This is what the GuiUnattended directive looks like in a remboot.sif file from Windows 2000:

```
[GuiUnattended]
AdminPassword=crackme
OEMSkipRegional=1
TimeZone=%TIMEZONE%
OemSkipWelcome=1
```

This is what the GuiUnattended directive looks like in a remboot.sif file from Windows 2003 server:

```
[GuiUnattended]
AdminPassword=a5c67174b2a219d1aad3b43
      5b51404ee363dd639ad34b6c5153c0f511
      65ab830
EncryptedAdminPassword=Yes
OEMSkipRegional=1
TimeZone=%TIMEZONE%
OemSkipWelcome=1
```

Now when that low-level user searches for this file, he/she will only find the encrypted password. This gives less experienced administrators a false sense of security.

The Issue

This is were the fun starts. All Microsoft has done is raise the bar a bit. If you know your hash, as I'm sure you do, you'll see this is a Lan Manager hash! This will keep your more remedial users at bay, but not the readers of *2600.*

I found if I reformatted the AdminPassword string and saved it to a new text file that I could feed it to my openMosix cluster running John the Ripper and, voila! I had the local Administrator password.

How To

The easiest way to format the hash is with the xpgrab utility.

#xpgrab remboot.sif

Say you have a kiddie bent on mischief. All he/she has to do is change the directive telling the setup program not to use encryption but to keep the encrypted string. This would look like this:
EncryptedAdminPassword=No

That way the new password would be the encrypted string, which would in all likelihood be more secure. This would make it hard for local administrators to say the least. This could also be a good way to own a network. You could also use Setup Manager to encrypt your favorite passwords so you can do a simple compare against the hash found on the server and the one you encrypted using Setup Manager. It would be slow, but hey, never say never.

Conclusion

Microsoft has gone to great lengths to protect the Lan Manager hash stored in the SAM and Active Directory. This is done with Syskey which encrypts this information using 128 bit key encryption. In the past you had to have an interactive login token (logged on to the server console), with administrator privileges and a tool like pwdump2.exe to get this information. The pwdump2 tool will not work if you are logged in via the remote desktop that has taken the place of the Windows 2000 Terminal Server remote administration mode. Leaving this key out defeats the very purpose of syskeying the SAM and Active Directory in the first place.

I hope this information will help the readers of *2600* as well as the hacking community.

Credits/Source

Solar Designer for John the Ripper
Microsoft Windows 2000 Server Administrator's Companion
Setup Manager online help
Todd Sabin for pwdump2
All of the hackers at the openMosix project
http://sourceforge.net
William T. Stafford and the rest of the cSd crew

```
# !/usr/bin/perl
# Script Name:xpgrab
# Script Version: 0.01
# Date: 02/27/2003
# Written by: Joseph B. Zekany (aka Zucchini)
# NOTE:
# If you are going to run this program in windoz add a .pl extension.
# For example (xpgrab.pl)
# Revision History:
# 0.01: Original Version
# --------------------------------------------------------------------------

$file = $ARGV[0];
if($file){
   open(FILE, "$file") || die "Could not open $file for reading please check if the
file exists:\n $!";
      @ info = <FILE>;
   close (FILE);
for ($i=0;$i<@info;$i++) {
   if ($info[$i] =~/\bAdminPassword/){
         @xphash = split("", $info[$i]);
         @xphash1 = @xphash[18 .. 49];
         @xphash2 = @xphash[50 .. 83];
         $xphash1 = join("", @xphash1);
         $xphash2 = join("", @xphash2);
         $xphash = "Administrator: 500:$xphash1:$xphash2\:::";
         open(HASH, ">xphash.txt") || die "Could not open file for writing: $!";
         print HASH $xphash;
         close (HASH);
         print "\n\nThe Lan Manager hash has been recovered, and is now\n";
         print "stored in a file named xphash.txt in the local directory.\n";
         print "It is now ready to be sent to John ";
         print "for further processing.;^)\n\n";
      }
   }
}else{
      print "Written by:\n\t\tJoseph B. Zekany\n";
      print "Date:\n\t\t02/27/03\n";
      print "Usage:\n\t\txpgrab <remboot.sif>\n\n";
}
```

How to mess with Citibank Collections

by The Pissed Off One Armed Man

OK, I bet you're thinking to yourself, why the heck would I want to mess with these folks? The answer: Citibank is *evil!*

Citibank has over 120 different types of "Private Label" cards, such as Rat Shack, Zales, Children's Place, Goodyear, Gateway, Helzburg Diamonds, and other fine merchants. Citibank even handles several oil cards as well, with brands such as Texaco, Shell, BP/Amoco/Boron, and Citgo. However, today we will discuss the oil card systems.

Citibank's collection centers for oil are located in Houston, Texas (collections only) (aka the Barker Cypress Center), Florence, Kentucky (collections only), and Des Moines, Iowa (customer service/payments).

Citibank uses a Windows NT based system for all of its collections and customer service activities. When a person logs into the system they use a generic Windows NT login and authenticate to the CARDS-NA domain. Generic logins can easily be obtained by walking the collections floor. After entering your login ID, you are taken to a blank desktop where six different applications automatically pop up. Magellan/Melita is their dialer system. It will prompt for a userid. Every associate in the bank is assigned an ID code in the format: AAAXXXX. The first three are the person's location. In Florence it was referred to as a CIN number. However, every location is different with these ID's.

Whenever you talk to an associate, be it for oil or for private label or for Mastercard/Visa collections, *get this number!* They are required to give it to you. If they give you another ID, tell them that they are full of shit. Also, ask for the center that they are calling from. They might give you a BP or BJ ID number as well. It will be in the form of BX10XXX where the last three are letters. The second digit depends on the product. Texaco and Shell use BJ ID numbers, BP and Citgo use BP ID numbers.

During the call they will try to act friendly towards you and try to gain your trust. Don't tell them shit. If you are only a few days late with a payment, *do not give it to them over the phone!* Every associate is driven by dollars collected and contacts per hour. Most collections reps from Citibank are only paid $9.25 to $10.25 per hour depending upon experience. Go take a look at http://careers.citicards.com.

The collectors in oil cards input data into a system known as CACS (or Computer Assisted Collections System). This application is housed next to the CCMS which stands for Credit Card Marketing System. This is the system that collections (limited access) and customer service (full access) use to service cardmember accounts. Each product has its own login command from starting screen. Every contact, be it a no answer, a busy, or an actual connect is noted within the system. If you use foul language against the collector, it is noted in the contact that the customer used foul language.

At the beginning of the call, get the operator's ID number. I can't stress this enough - it will come in handy. Collectors are also guided on customer feedback as well. You should do whatever you can to make them hang up on you. Then take that ID number you were given in the beginning and give customer service a call. If you're in collections, *do not enter* your account number when the IVR comes up. Just wait... it will eventually transfer you to a customer service representative. Tell the customer service representative that you'd like to speak to a manager. If they give you a problem about it, demand the manager right then and there. Make up a story about how you were trying to discuss the account rationally with the collector and the collector hung up on you. That is forbidden by policy. When they pull your account, they'll see a note written by the collector revealing what you said or did on the phone. Tell them that it is bullshit, and they will also counsel the employee on Falsification of Bank Documents.

Citi almost always takes the word of the customer over the word of the employee. Now, assuming that the representative wasn't monitored (which rarely happens) Citi will kiss your ass to try to save your account. You can work out all kinds of interesting deals with them. Ask about REAGE (which means in English that if you pay a certain amount on the account, your account will be brought current), CAP (Customer Assistance Program - can be done anywhere from 3-12 months), or a settlement.

I remind everyone that this information is for educational purposes only and I am not responsible if you get some odd person knocking at your door. Oh, and also, Citibank's employment policy is Employment at Will. Some of these managers are nazis towards their people.

Marketplace

Happenings

THE FIFTH HOPE will take place at New York City's Hotel Pennsylvania from July 9th to the 11th. This will be a very special conference, marking the 20th anniversary of *2600* and the 10th anniversary of the First Hope. We're currently organizing speakers, network setup, and more. If you want to get involved, check www.hope.net frequently as we'll be posting updates on an ongoing basis.

INTERZ0NE III. April 2004. Not just another hackers' con! Stay tuned to website for more details. www.interz0ne.com (that's a zero!)

For Sale

CABLE TV DESCRAMBLERS. New. (2) Each $74 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaleton Internet provides affordable web hosting based on Linux servers. Our hosting plans start from only $4.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. Privacy is guaranteed and you can pay by E-Gold, paypal, or credit card. http://www.kaleton.com

DRIVER'S LICENSE BAR-BOOK and "fake" ID templates. Includes photos, templates, and information on all security features of every single American and Canadian drivers' licenses. Including information on making "fake" ID's on PVC cards, laminating, making holograms, magnetic stripes, software, and more to make your very own license! Send $25 cash in US funds or an international money order in US funds made out to R.J. Orr and mailed to Driver's Bar Book, PO Box 2306, Station Main, Winnipeg, Manitoba, R3C 4A6, Canada. Order now and get FREE laminates with every order! We ship worldwide free!

ONLINE RETAILER OF COMPUTER PRODUCTS is also a *2600* subscriber! 60,000 different computer products from components to complete systems, laptops, PDAs, cables, RAM, and media all available online at http://www.digitaleverything.ca. Worldwide shipping is no problem. Just mention you are a subscriber and I'll give you better prices too. Contact Dave at sales@digitaleverything.ca for more info.

AT LAST AN ACCURATE DESCRIPTION OF THE BELIEFS AND BEHAVIOR OF HACKERS! Social Inquiry offers a research report produced by Bernhardt Lieberman, emeritus professor from the University of Pittsburgh and Director of Social Inquiry, his own social research firm. Professor Lieberman held appointments in the Departments of Sociology and Psychology at the University of Pittsburgh. He conducted a detailed interview of hackers in Pittsburgh and administered five questionnaires to them: a hacker motivation questionnaire, a hacker ethic questionnaire, an attitude toward the law scale, a liberalism-conservatism scale, and a personality questionnaire designed to deal with the myth of the hacker as a social misfit. Professor Lieberman attended H2K2, observed the behavior of hackers in convention, and administered the five questionnaires to hackers attending H2K2. The report also contains a content analysis of *2600.* The report presents a description of the beliefs and behavior of hackers produced by these methods of inquiry. The report is neither a condemnation nor a whitewash of hackers, nor does it justify the actions of criminal justice systems and the disciplinary actions of school administrators. It is designed to offer a more accurate picture of hackers than the pictures presented by the mass media and the criminal justice systems. The report recommends that the desire of hackers to learn about computers, computing, and technology should be channeled into constructive ends, as much as that is possible. The report is 140 pages long and contains 55,000 words. Professor Lieberman received no grant or contract money to do this work; he did the work using his own money and was, and is, beholden to no one. To get a copy of the report send a check or money order for $23.50 + $4.50 ($6.00 outside North America) for shipping (in U.S. dollars) payable to Social Inquiry, 627 Beverly Road, Pittsburgh, PA 15243. Those fortunate enough to have institutional funds to pay for the report are invited to send a purchase order. Professor Lieberman can be reached at 412.343.2508. His website is www.telerama.com/~blieber.

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $16.95 + $1.55 S/H. Mail order to: P.H., 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

SIZE *DOES* MATTER! The Twin Towers may be gone forever but a detailed image still exists of the massive 374-foot radio tower that was perched atop One World Trade Center. This high-quality glossy color poster is available in two sizes (16" x 20" and 20" x 30") and makes a spectacular gift for engineers, scientists, radio and television buffs, or anybody who appreciates a unique, rarely seen view of the World Trade Center. Visit www.wtc-poster.us for samples and to order your own poster.

WIRELESS SECURITY PERSPECTIVES. Monthly, commercial-grade information on wireless security. Learn how to protect your cellular, PCS, 3G, Bluetooth, or WiFi system from *2600* readers. Subscriptions start at $350 per year. Check us out at http://cnp-wireless.com/wsp.html.

TAP/YIPL The original phreaking and hacking zines! All original back issues on CD-ROM. Only $5 including postage! Write for a free catalog of the best underground CD-ROMS! Whirlwind, Box 8619, Victoria BC, V8W 3S2, Canada.

LEARN LOCK PICKING It's EASY with our book. Our new edition adds lots more interesting material and illustrations. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your 2600 reader price discount.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $49.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

WORLD'S FIRST "DIGITAL DRUG." Hackers, get ready to experience the next level in wetware technology! VoodooMagickBox is a 100% legal and safe way to enter into a drug-like trip, All you need to do is place the clips on your ears and turn the knob on the VoodooMagickBox. It's like nothing you've ever tried! For details and ordering information, visit www.voodoomagickbox.com (money orders and credit cards accepted).

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $3 cash to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

Help Wanted

CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

NEED ASSISTANCE to rescue/recover ASCII text data which are presently compressed/encrypted by some type of commercial program. Most files are rather large, from 30MB to about 600MB. Using DOS based search engine for retrieval. Please advise if there exists any tools currently available or anyone who may be of help. johndp4@hotmail.com.

Wanted

SEEKING MANUSCRIPTS FOR PUBLICATION. The Paranoid Publications Group is currently accepting unsolicited, unpublished manuscripts for consideration. For complete information, download our electronic author's information package by visiting www.paranoidpublications.com and clicking on "Authors." While you're there, check out our newest book - *The Preparatory Manual of Chemical Warfare Agents.* Author Jared B. Ledgard shows us how to prepare and handle numerous hazardous chemical substances of a hazardous nature. Written in plain English, this manual is simple enough for the common man to comprehend yet advanced enough to hold the attention of even the most accomplished chemist. Enter coupon code "winter2600" (without the quotes) for 10% off your order. Visa, MasterCard, American Express, Discover, JCB, and old fashioned checks and money orders are welcomed. No orders by telephone, please. Customer service and product information: 800-681-8995.

BUYING BOOKS AND MORE. Man interested in books related to hacking, security, phreaking, programming, and more. Willing to purchase reasonable books/offers. I do search Google! No rip-offs please. Contact me at lbda@att.net.

FREE SOFTWARE DISTRIBUTION. I have a website (www.eloder.com, come check it out!) that has a fair amount of traffic. Mostly for debian and redhat cds. I am looking for hackers who have made their own interesting programs and wish to share. If you have some really interesting apps, I can give you (for free!) a page or a sub domain. I am looking to assist the open source movement and the hacker community. You can email me at eloder@hotmail.com. Please place "download" in the subject heading. All interesting ideas welcome. Eric Loder.

NEED DIAL UP HACKING INFO (steps involved, current dial ups, etc.) Also looking for places on the Internet where I can get unlisted phone numbers for free. Please contact me at billm2@prodigy.net.

THE NEW YORK CITY INDEPENDENT MEDIA CENTER (NYC-IMC) is looking for donations to help build an IU server to host its open publishing web site. NYC-IMC (http://nyc.indymedia.org) is an all volunteer collective and is part of a worldwide network of over 100 media centers (http://www.indymedia.org) dedicated to maintaining an open publishing web system covering progressive issues and built using open source technologies. NYC-IMC has outgrown its current server and host and would like to create a robust, rack mountable server that can be collocated with a faster provider. If you can donate time or parts to help build our server, please get in touch with the NYC-IMC Tech Team at imc-nyc-tech@indymedia.org.

SEEKING INFORMATION ABOUT TRACFONE. Looking for technical data concerning the Tracfone network and how it operates, especially information about airtime and the manipulation thereof. I have been working for some time to compile an extensive tutorial about Tracfone and how its service works and I am currently working on the fourth revision. The third revision and quite a little bit of information that I have already discovered on my own can be found at www.americasleastwanted.com in the Scams & Fraud section of the site. Send any information via e-mail to tracfone-response@americasleastwanted.com. I will not pay for information and you shouldn't want to charge for it because that would be against your hacker ethics. Or something. I am also looking for people to write tutorials and other content on this site as well. Contact webmaster@americasleastwanted.com if you are interested. These will also be unpaid positions.

IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tactics." But it doesn't work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

Services

VINTAGE COMPUTER RESOURCES FOR RESEARCH. VintageTech provides a wide variety of computer historical related services for business and academia. We provide: support services for legal firms for computer and software patent litigation and prior art research; props and consulting for movie or film production and photography studios requiring period authentic computers and computer related items; data recovery and conversion from old and obsolete data media to modern media; appraisals of vintage computer items for sale, charitable donation, or insurance valuations; sales brokering of vintage computers and related items; general computer history consulting and research. VintageTech maintains an extensive archive of computers, software, documentation, and an expansive library of computer related books and magazines. Visit us online at http://www.vintagetech.com or call +1 925 294 5900 to learn more about the services we provide.

PAY2SEND.COM is an e-mail forwarding service that only forwards messages from whitelisted contacts or people who pay you to receive from them, using a patent-pending identity technique. Sign up via our web page form.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, without big-brother looking over their shoulder. We provide highly filtered DoS protection. Our main server is a P3 1.2 ghz machine, 1.5 gigs of ram, 512 megs of swap, 40 gig EIDE, with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.

HACKERSHOMEPAGE.COM. Your source for keyboard loggers, gambling devices, magnetic stripe reader/writers, vending machine defeaters, satellite TV equipment, lockpicks, etc... (407) 650-2830.

CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

HACKERMIND: Dedicated to bringing you the opinions of those in the hacker world, and home of the ezine *Frequency.* Visit www.hackermind.net for details.

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer viruses. The White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.

Personals

STORMBRINGER'S 411: My Habeas Corpus (2255) was just denied so I'm in for the 262 month long haul. Am trying to get back in contact with the D.C. crew, Roadie, Joe630, Alby, Protozoa, Ophie, Professor, Dr. Freeze, Mudge, VaxBuster, Panzer, and whoever else wants to write. P.T. Barnum, I lost your 411. Wireless, ham, data over radio is my bag. Write: William K. Smith, 44684-083, FCI Cumberland Unit A-1, PO Box 1000, Cumberland, MD 21501 (web: www.stormbringer.tv).

PRISON SUCKS! Help me pass the time in here and write to me. Only 2 more years left and I am going crazy without any mental stimulation. I welcome letters from anyone and will reply to each and every one. Jeremy Cushing #J51130, Centinela State Prison, P.O. Box 911, Imperial, CA 92251.

RESOURCE MAN is looking for more addresses (snail mail). Please send any addresses of the following: book clubs, subscription services, newspapers, computer/hacking magazines, and any foreign addresses which are a special delight. The further away the better. Also, I am a manga/anime fanatic (dbz, Digimon, Outlaw Star, Chobits, Tenchi Muyo, etc.). Please send any related information to: Daniyel Sigsworth #1062882, PO Box 2000, Colorado City, TX 79512. Will respond if desired.

AN INTERESTED "TO-BE" HACKER IN PRISON: I am a 28 year old in prison who is interested in learning on being a hacker. I'm looking to hear from anyone who can help me get started on being a hacker, for advice, and to correspond with on anything doing with hacking. Please help an up and coming to be hacker out. I will correspond with anyone. Write to me at: Michael Engebretson #245523, Prairie Correctional Facility, PO Box 500, Appleton, MN 56208.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Spring issue: 3/1/04.

Meetings

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.
Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.
Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.
Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.
Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.
Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.
Victoria: Eaton Center food court by A&W.

Manitoba

Winnipeg: Garden City Shopping Center, Center Food Court adjacent to the A & W restaurant.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 143 Pembroke Street West. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.
Guelph: William's Coffee Pub, 429 Edinbourgh Road. 7 pm.
Hamilton: McMaster University Student Center, Room 318, 7:30 pm.
Ottawa: Agora Bookstore and Internet Cafe, 145 Besserer Street. 6:30 pm.
Toronto: Food Bar, 199 College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Ved Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm.

ENGLAND

Exeter: At the payphones, Bedford Square. 7 pm.
London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.
Manchester: The Green Room on Whitworth Street. 7 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.
Grenoble: McDonald's south of St. Martin d'Heres.
Paris: Place de la Republique, near the (empty) fountain. 6 pm.
Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

IRELAND

Dublin: At the phone booths on Wicklow Street beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.
Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.
Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.
Tromsoe: The upper floor at Blaa Rock Cafe. 6 pm.
Trondheim: Rick's Cafe in Nordregate. 6 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SLOVAKIA

Bratislava: at Polus City Center in the food court (opposite side of the escalators). 8 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: Outside Vanilj. 6 pm.
Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.
Huntsville: Madison Square Mall in the food court near McDonald's. 7 pm.
Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Borders, 2nd Floor Cafe Area, 2402 E. Camelback Road.
Tucson: Borders in the Park Mall. 7 pm.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.
Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.
San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.
Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

District of Columbia

Arlington: Pentagon City Mall in the food court. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.
Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.
Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Union Station in the Great Hall near the payphones.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.
Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.
Indianapolis: Borders Books on the corner of Meridian and Washington.
South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Santa Fe Espresso, 116 Welch Ave.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.
New Orleans: La Fee Verte, 620 Conti Street. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows.
Marlborough: Solomon Park Mall food court.
Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.
St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.
Springfield: Barnes & Noble on Battlefield across from the mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Palms Casino food court. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

Buffalo: Galleria Mall food court.
New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court.
Greensboro: Four Seasons Mall Food Court (in the back). 6 pm.
Raleigh: Crabtree Valley Mall food court in front of the McDonald's.
Wilmington: Independence Mall food court.

North Dakota

Fargo: Barnes and Nobles Cafe on 42nd St.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.
Cincinnati: Cody's Cafe, 113 Calhoun St., far back room. 6 pm.
Cleveland: University Circle Arabica.
Columbus: Convention Center (downtown), south (hotel) half, carpeted payphone area, near restrooms, north of food court. 7 pm.
Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: The Magic Lamp in the Lakeside Shopping Center near the corner of N. May Ave. and NW 73rd St.
Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Heaven Cafe, 421 SW 10th Ave., near 10th and Stark.

Pennsylvania

Allentown: Panera Bread on Route 145 (Whitehall). 6 pm.
Philadelphia: 30th Street Station, under Stairwell 7 sign.
Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.
Memphis: Cafe inside Bookstar - 3402 Poplar Ave. at Highland. 6 pm.
Nashville: J-J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court.
Dallas: Mama's Pizza, Campbell & Preston. 7 pm.
Houston: Cafe Nicholas in Galleria 1.
San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)
Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

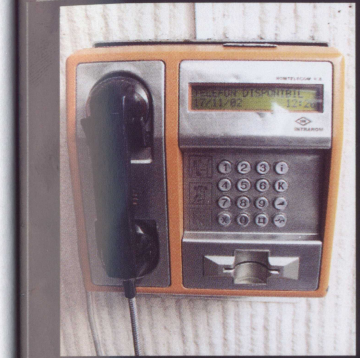
Seattle: Washington State Convention Center. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Copper Hearth Lounge.
Milwaukee: The Node, 1504 E. North Ave.

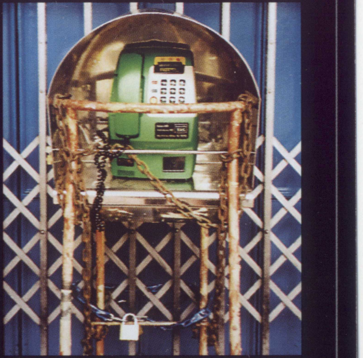
All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Payphones From All Around The World



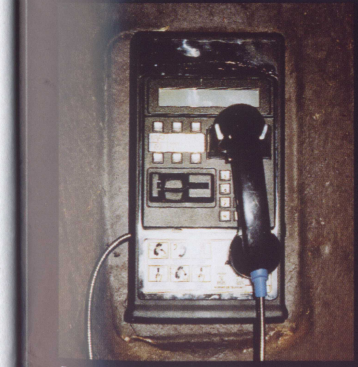
Romania. One of the more modern phones useful for telling you the date and time among other things. And it's orange!

Photo by Dieter K.



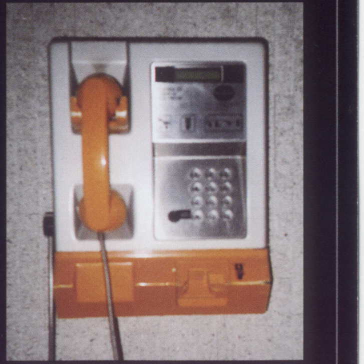
Singapore. So much for the perfect society. Apparently payphone theft is still a popular activity.

Photo by Louis Pezzani



Paraguay. Located in the Monday State Park near the Monday Falls in Ciudad del Este.

Photo by Darryl Duer



Colombia. Found in the airport of Barranquilla. We just don't see enough orange phones.

Photo by Bruce Engelberg

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com